SMC®
Networks

SMC2804WBRP-G
Barricade™ g 2.4 GHz Wireless Router with USB Print Server

USER GUIDE

Copyright
Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Trademarks:
SMC is a registered trademark; and Barricade is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

TABLE OF CONTENTS

CHAPTER 1 | Introduction

Congratulations on your purchase of a Barricade™ g Broadband Router with USB Print Server (SMC2804WBRP-G). SMC is proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet and sharing a USB printer on your network.

1.0 | Features and Benefits

- **EZ 3-Click Installation Wizard -** A new and improved way to install your Barricade in seconds
- Built-in USB print Server to share your USB-enabled printer
- Internet connection to ethernet broadband modem via a 10/100 Mbps WAN port
- Local network connection via a 4-port auto-sensing 10/100 Mbps Ethernet switch
- DHCP for dynamic IP configuration, and DNS for domain name mapping
- Firewall with Stateful Packet Inspection, client privileges, hacker prevention, DoS, and NAT
- NAT also enables multi-user access with a single-user account, and virtual server functionality (providing protected access to Internet services such as web, mail, FTP, and Telnet)
- Virtual Private Network support using PPTP, L2TP, or IPSec pass-through
- User-definable application sensing tunnel supports applications requiring multiple connections
- Parental controls allows the user to block access to certain web sites
- Email alerts when the users network is being compromised
- Easy setup through a web browser on any operating system that supports TCP/IP
- Compatible with various internet applications, including Peer-to-Peer file sharing, Online Games, and Instant Message utilities.

1.1 | Package Contents

Before installing the Barricade™ g Broadband Router with USB Print Server, verify that you have the items listed under "Package Contents." Also be sure that you have the necessary cabling. If any of the items are missing or damaged, contact your local SMC distributor.

- Barricade g Broadband Router with USB Print Server
- Power adapter (9v/1a)
- One CAT-5 Ethernet cable
- CD with User Guide and EZ 3-Click Installation Wizard
- Quick Installation Guide

If possible, retain the carton and original packing materials in case there is a need to return the product.

1.2 | Minimum Requirements

- Cable or DSL Modem with Ethernet connection and Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem or cable modem.
- A computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or USB-to-Ethernet converter.
- Network adapter with Ethernet (UTP CAT 5) cabling and TCP/IP protocol installed per PC
- Internet Explorer 4.0 (or Higher) or Netscape Navigator 4.7 (or Higher) for Web-based configuration of the Barricade

CHAPTER 2 | Getting to Know the Barricade

The SMC2804WBRP-G Barricade Cable/DSL Broadband Router is the perfect solution for the home/office environment. This full-featured router offers:

- 1 - USB 1.1 Print Server port
- 802.11g Wireless with Performance Enhancing Nitro™ Technology
- 4 - 10/100 Mbps Auto-Sensing LAN ports with Auto-MDI MDIX feature
- 1 - 10/100 Mbps WAN port with Auto-MDI MDIX feature
- Comprehensive LEDs for network status and troubleshooting
- Reset Button

2.1 | LED Indicators

The Barricade includes LED indicators on the front panel that simplify installation and network troubleshooting.

LED	ON	OFF	FLASHING
PWR (POWER)	Receiving power	Not receiving power	N/A
SPD (WAN)	100Mbps WAN connection detected	10Mbps WAN connection detected	N/A
Link/ACT (WAN)	Good WAN connection detected	No WAN connection detected	Data transmitting through the WAN
WLAN	Wireless function is enabled	Wireless function is disabled	Data transmitting through wireless
Link/ACT (LAN)	Good LAN connection detected	No LAN connection detected	Data transmitting through the LAN

Resetting the Barricade
The Reset button is located on the rear panel of the Barricade Broadband Router. Use a paper clip or a pencil tip to push the Reset button.

Reset
If the Router is having problems connecting to the Internet, simply unplug the router for 3 seconds then plug back in.

Restore Factory Defaults
If resetting the router does not resolve your issue, then you can follow these steps:

1. Leave power plugged into the router
2. Locate the reset button on the back panel, press and hold until WAN LED flashes off.
3. Release reset button.

CHAPTER 3 | Getting Connected

The SMC2804WBRP-G Barricade g Router with USB Print Server is connected between the Ethernet Broadband Modem and your computers, either wired or wireless. If you have more then one computer to connect, simply plug the other computers into the LAN ports on the back of the router or connect via a wireless signal.

3.1 | Basic Installation Procedure

1. **CONNECT the WAN**
   Connect an Ethernet cable from your cable or DSL modem to the Barricade g WAN port on the back on the router.

2. **CONNECT the LAN**
   Run an Ethernet cable from one of the LAN ports on the back of the Barricade g to your computer's wired network adapter.

3. **POWER on**
   Connect the power cable to the Barricade.

NOTE: It is highly recommended that you do you initial configuration from a wired connection.

Once you have completed connecting all of the hardware, simply insert the Barricade g CD-ROM and the **EZ 3-Click Installation Wizard** will automatically get you connected you to the Internet.

For manual configuration of the PCs, see Chapter 4.

For advanced configuration of the Barricade Broadband Router, see Chapter 5.

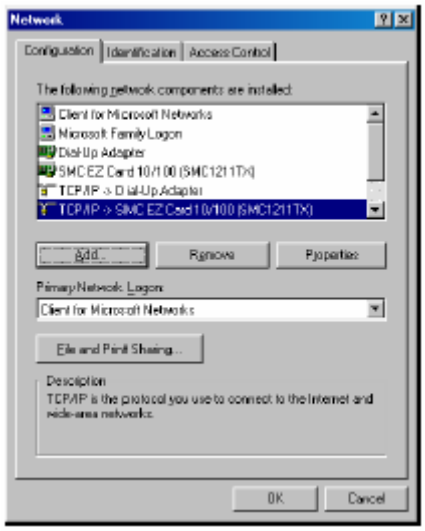
CHAPTER 4 | Configuring your Computer

The information outlined in this chapter will guide you through the configuration for the following Operating Systems:

- Windows 95/98
- Windows Me
- Windows 2000
- Windows XP
- Apple Macintosh

4.1 | Configuring Windows 95/98/Me

1. Access your Network settings by clicking [Start], choose [Settings], and then select [Control Panel].
2. In the Control Panel, locate and double-click the [Network] icon.



3. Highlight the TCP/IP line that has been assigned to your network card on the [Configuration] tab of the [Network] properties window.
4. Next, click the [Properties] button to view that adapter's TCP/IP settings.

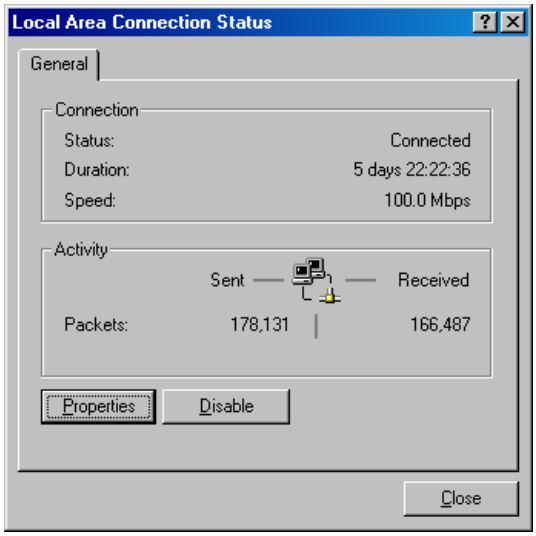
5. From the TCP/IP Properties dialog box, click the [Obtain an IP address automatically] option.
6. Next click on the [Gateway] tab and verify the Gateway field is blank. If there are IP addresses listed in the Gateway section, highlight each one and click [Remove] until the section is empty.
7. Click the [OK] button to close the TCP/IP Properties window.
8. On the Network Properties Window, click the [OK] button to save these new changes.

   NOTE: Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, for example, D:\win98, D:\win9x. (assume "D" is your CD-ROM drive).

9. Windows may prompt you to restart the PC. If so, click the [Yes] button. If Windows does not prompt you to restart your computer, do so anyways to ensure your settings.

4.2 | Configuring Windows 2000

1. Access your Network settings by clicking [Start], choose [Settings], and then select [Control Panel]
2. In the Control Panel, locate and double-click the [Network and Dial-up Connections] icon
3. Locate and double-click the [Local Area Connection] icon for the Ethernet adapter that is connected to the Barricade. When the Status dialog box window opens, click the [Properties] button.

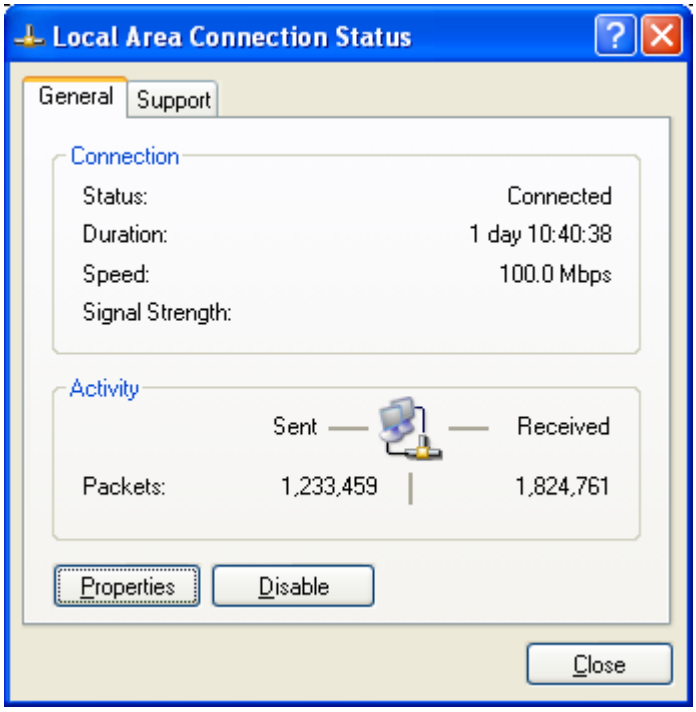


4. On the [Local Area Connection] Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
5. Select Obtain an IP address automatically to configure your computer for DHCP. Click the [OK] button to save this change and close the Properties window.
6. Click the [OK] button again to save these new changes.
7. Reboot your PC.

4.3 | Configuring Windows XP

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000 outlined above.

1. Access your Network settings by clicking [Start], choose [Control Panel], select [Network and Internet Connections] and then click on the [Network Connections] icon.
2. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Barricade Router. Next, click the [Properties] button.



3. On the [Local Area Connection] Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
4. Select Obtain an IP address automatically to configure your computer for DHCP. Click the [OK] button to save this change and close the Properties window.
5. Click the [OK] button again to save these new changes.
6. Reboot your PC.

4.4 | Configuring a Macintosh Computer

You may find that the instructions here do not exactly match your screen. This is because these steps and screenshots were created using Mac OS 8.5. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 8.5.

1. Pull down the Apple Menu. Click [Control Panel] and select TCP/IP.
2. In the TCP/IP dialog box, make sure that [Ethernet] is selected in the [Connect Via:] field.

   If [Using DHCP Server] is already selected in the [Configure] field, your computer is already configured for DHCP. Close the TCP/IP dialog box, and skip to Step 2 Disable HTTP Proxy (bottom of this page).

3. All the information that you need to record is on the [TCP/IP] dialog box. Use the space below to record the information.
4. Select [Using DHCP Server] in the [Configure] field and close the window.
5. Another box will appear asking whether you want to save your TCP/IP settings. Click [Save].

CHAPTER 5 | Configuring the Barricade

After you have configured TCP/IP on a client computer, use a web browser to configure the Barricade™ Broadband Router. The Barricade can be configured by any Java-supported browser including Internet Explorer 4.0 or above, or Netscape Navigator 4.7 or above. Using the web management interface, you may configure the Barricade and view statistics to monitor network activity.

> **NOTE**: Before you attempt to configure your router, if you have access to the Internet please visit www.smc.com and download the latest firmware update.

Before you attempt to log into the Barricade's Web-based Administration, please verify the following:

1. Your browser is configured properly. (see below)
2. Disable any firewall or security software that may be running.
3. Confirm that you have a good "link" LED where your computer is plugged into the Barricade. If you don't have a "link" light, try another cable until you get a good link.

5.1 | Browser Configuration
Confirm your browser is configured for a direct connection to the Internet using the Ethernet cable that is installed in the computer. This is configured through the options/preference section of your browser.

5.2 | Disable Proxy Connection
You will also need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your web browser will be able to view the Barricade configuration pages. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer (5 or above)

1. Open Internet Explorer. Click [Tools], and then select [Internet Options].
2. In the [Internet Options] window, click the [Connections] tab.
3. Click the [LAN Settings] button.
4. Clear all the check boxes and click [OK] to save these LAN settings changes.
5. Click [OK] again to close the [Internet Options] window.

Netscape (4 or above)

1. Open Netscape. Click [Edit], and then select [Preferences].
2. In the [Preferences] window, under [Category], double-click [Advanced], then select the [Proxies] option.
3. Check [Direct connection to the Internet].
4. Click the [OK] button to save the changes.

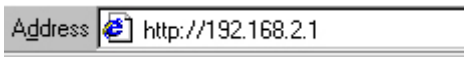
5.3 | Accessing the Barricade Management

To access the Barricade's web-based management screens, follow the steps below:

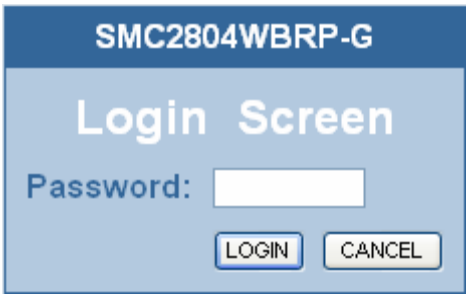
1. Launch your web-browser.

   NOTE: Your computer does not have to be ONLINE to configure the Barricade Router.

2. In the Address Bar, type: http://192.168.2.1



3. When the Barricade's Login screen appears, enter the default password, and click the [Login] button to access the router.



   NOTE: The Barricade g default password is "**smcadmin**". The password is case sensitive.

4. Once you have logged into the Barricade web-based admin screens, you have 2 options which are outlined in **Chapter 6 | Navigating the Web-based Administration**

CHAPTER 6 | Navigating the Web-based Administration

The Barricade's management interface features a Setup Wizard and an Advanced Setup section. Use the Setup Wizard if you want to quickly setup the Barricade for use with a cable modem or DSL modem. Advanced setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, intrusion detection, virtual server setup, virtual DMZ hosts, as well as other advanced functions.

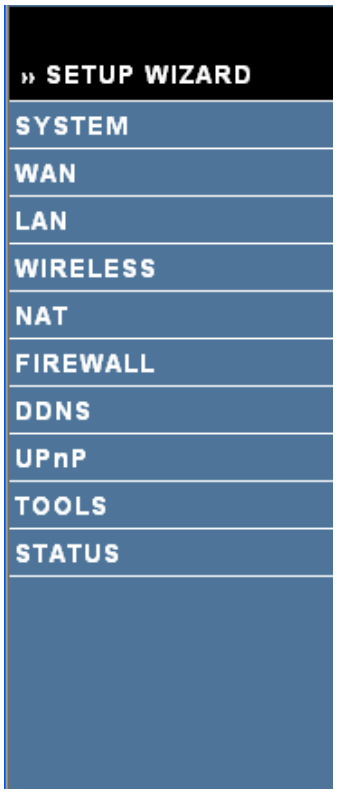
6.1 | Making Configuration Changes

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the "SAVE SETTINGS" or the appropriate button at the bottom of the page to save and enable the new settings.

Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the menu "Tools/Internet Options/General/Temporary Internet Files/Settings," the setting for "Check for newer versions of stored pages" should be "Every visit to the page."

This next generation Barricade has a new web-based interface that is easier to use and is faster. Each option is accessible from the new side navigation section.

If you want to setup the Router using the built-in Setup Wizard, simply click on the SETUP WIZARD option to start the process.

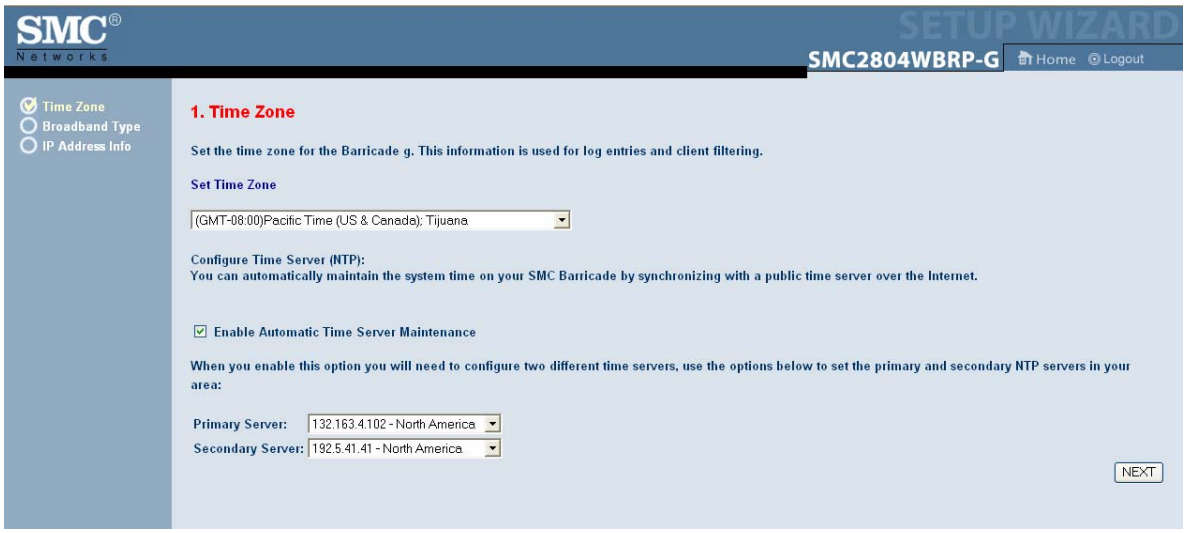


CHAPTER 7 | Setup Wizard

Below is an outline of each option available from the Setup Wizard section. This wizard takes 3 steps to complete an ISP configuration.

7.1 | Step One: Time Zone

The first step is to configure the Time Zone you are located in. This setting is used for accurate timing of client filtering and log events.



7.2 | Step Two: Broadband Type

Select the type of broadband connection you have.

Cable Modem: This is a Dynamic or DHCP Internet connection type – typically used by Cable Modem Internet connections.

Fixed-IP xDSL: This is a Static IP Internet connection type – choose this option if you ISP has provided you with all the correct static IP info.

PPPoE: This Internet connection method requires a username and password - typically used by xDSL Internet connections.

PPTP: Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.

BigPond®: The BigPond Internet service is used in Australia and uses a Heartbeat client to stay online.

7.3 | Step Three: Finish Configuration

Once you have configured your type of ISP connection, simply click the [Finish] button and the Barricade g will automatically configure your Internet connection.

CHAPTER 8| Advanced Setup

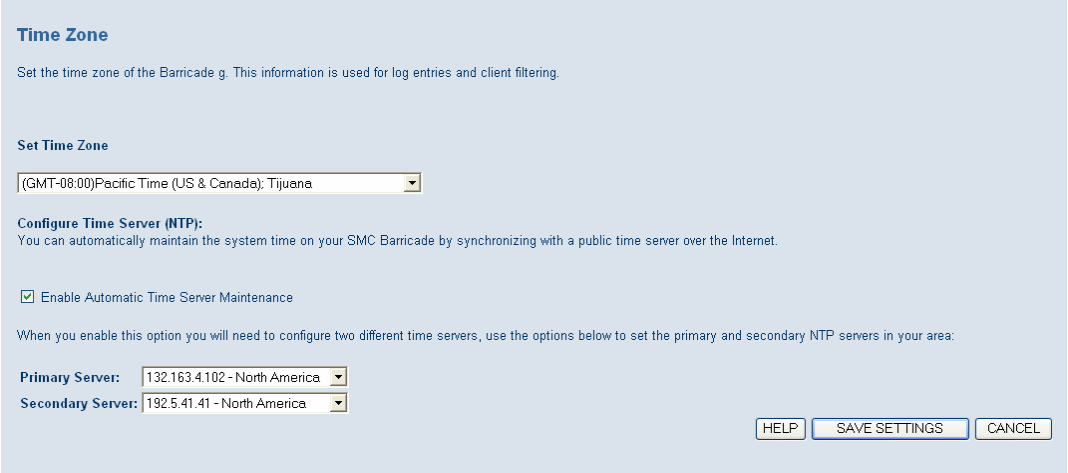
Below is an outline of the Advanced Setup section. This section is used to manually configure your ISP connection and also define the advanced system parameters, manage and control the Barricade and its ports, or monitor network conditions.

8.1 | System

This section is used to configure the local time zone, password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade remotely.

8.1.1 | Time Zone

Use this option to configure the time zone for the Barricade. This information is used for log entries and client access control.



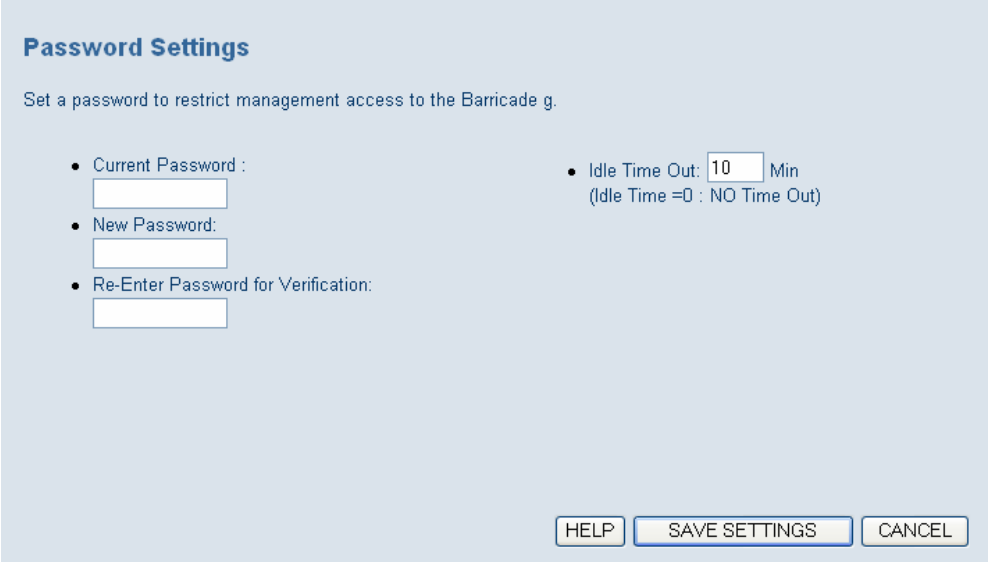
In this section you can enable or disable the Automatic Time Server Maintenance feature. This features uses open-access NTP servers available on the internet to keep your Router Time/Date current.

For the best results, choose a Primary Server and Secondary Server. If the Barricade is unable to reach the Primary Server for any reason (i.e. busy) then it will default to the Secondary Server.

8.1.2 | Password Settings

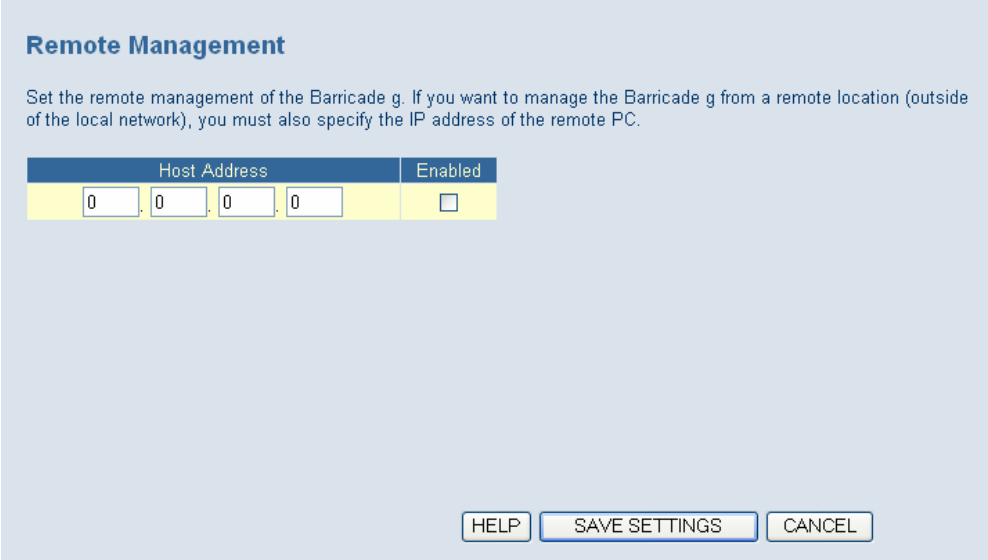
Use this menu to restrict access based on a password. By default, the password is "smcadmin".

NOTE: Passwords can contain up to 9 alphanumeric characters and are case sensitive.



8.1.3 | Remote Management

This feature allows a remote PC to configure, manage, and monitor the Barricade using a standard web browser.



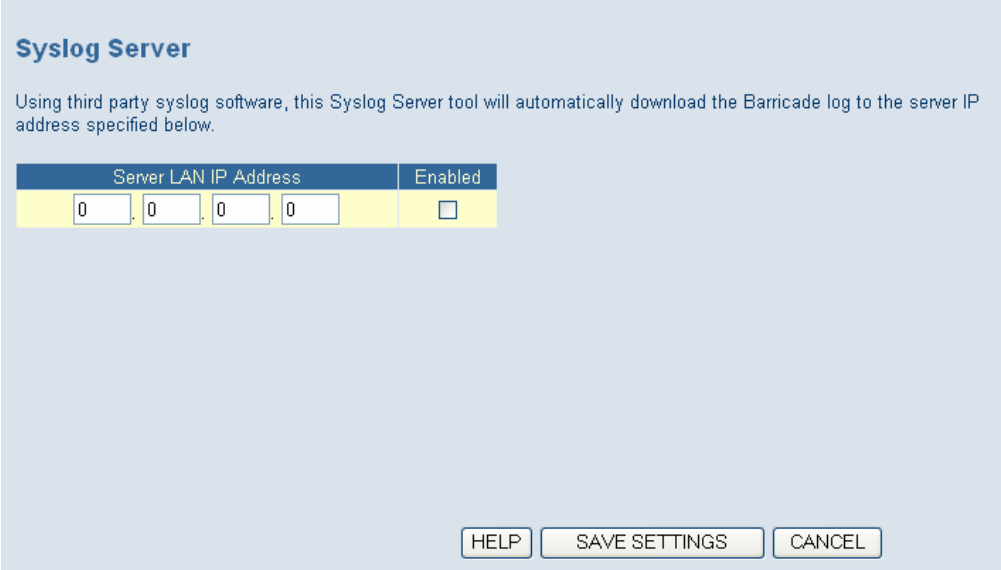
The default port for WAN remote management is port 8080.

To access the Barricade remote management from the Internet you can use any web browser. To access it follow this format for the URL:

http://xxx.xxx.xxx.xxx:8080 (xxx.xxx.xxx.xxx = your WAN IP address)

8.1.4 | Syslog Server

Use this feature to export Barricade Log information directly to a PC on your network.



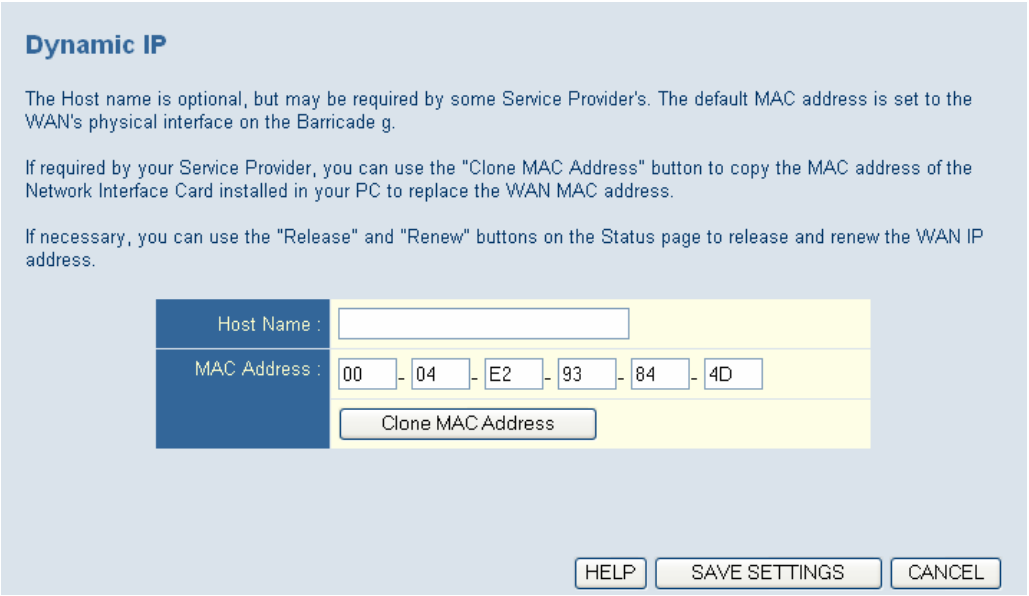
There are several shareware applications that you can use with this feature, such as the one available from www.kiwisoftware.com.

8.2 | WAN

In this section you will specify the Internet connection type that you are using, once you choose Internet option you are using click [More Configuration] button to enter detailed configuration parameters for the selected connection type.

8.2.1 | Dynamic (DHCP) IP

The Default Internet Connection type is Dynamic or DHCP IP. Most cable modem ISPs use this type of connection.



Host Name: The Host Name is optional, but it may be required by some ISPs.

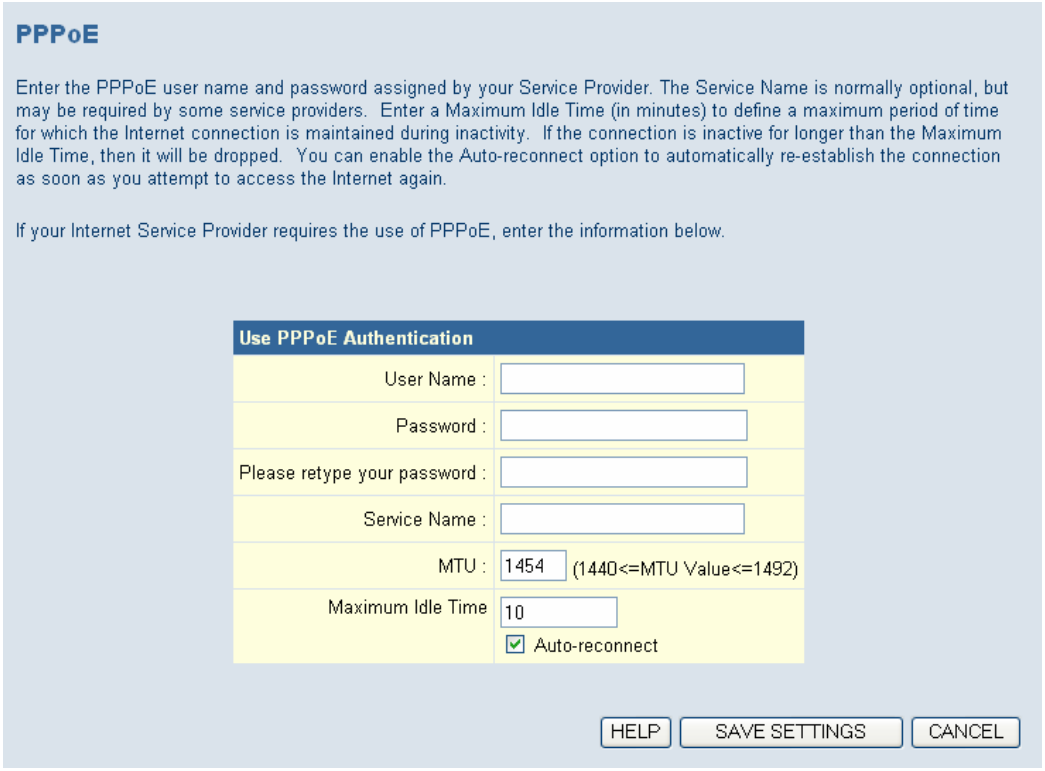
MAC Address: A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Barricade by clicking the [Clone MAC Address] button.

NOTE: If you are unsure of which PC the broadband connection originally set up, contact your ISP and request they register a new MAC address for your account. Register using the Barricade's MAC address which can be found on the STATUS page.

Need some more help?
If you are having problems getting online with your Dynamic IP connection, please refer to **Appendix B | Troubleshooting Internet Connections**.

8.2.2 | PPPoE

Some DSL ISPs require a username and password to get online. This type of connection method is called PPPoE or Point-to-Point Protocol over Ethernet. If you have been assigned a username and password from your ISP then you will use this Internet connection option.



Username and Password: Enter the PPPoE user name and password assigned by your Internet Service Provider.

Service Name: The Service Name is normally optional, but may be required by some service providers.

MTU: The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1492) unless you have a particular reason to change it.

Connect on Demand: Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped.

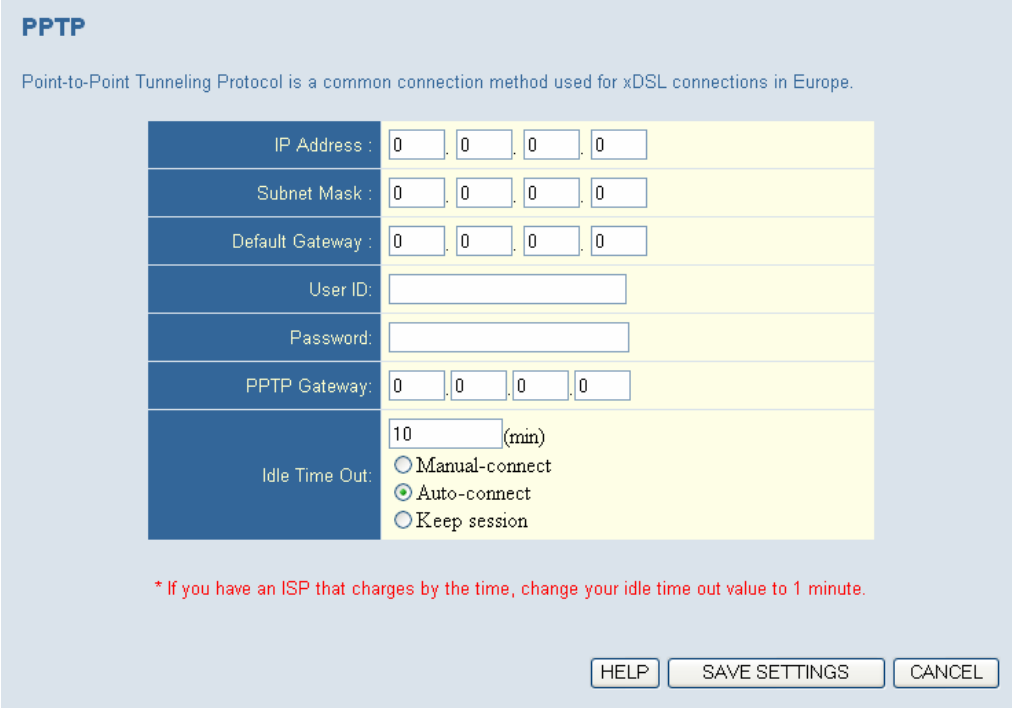
When checked, the [Auto-reconnect] option will automatically re-establish the connection when an application attempts to access the Internet again.

WARNING: If you are using an ISP that charges based on the amount of time that you are online, disable the Auto-Reconnect option and set your Max Idle Time to 2 minutes.

Need some more help?
If you are having problems getting online with your PPPoE connection type, please refer to **Appendix B | Troubleshooting Internet Connections**.

8.2.3 | PPTP

Point-to-Point Tunneling Protocol (PPTP) allows the secure remote access over the Internet by simply dialing in a local point provided by an ISP. This Internet connection type is mostly used in Europe.



IP Address: This is information will be provided by your ISP. If you do not have it please contact them.

Subnet Mask: This is information will be provided by your ISP.

Default Gateway: This is information will be provided by your ISP.

Username ID and Password: Enter in the username and password information provided by your ISP.

Connect on Demand: Idle Time Out. You can configure the Barricade to disconnect the connection after it has been inactive for a defined amount of time.

Manual-connect: This option will require that you click the [Connect] button on the status page after the connection has timed out.

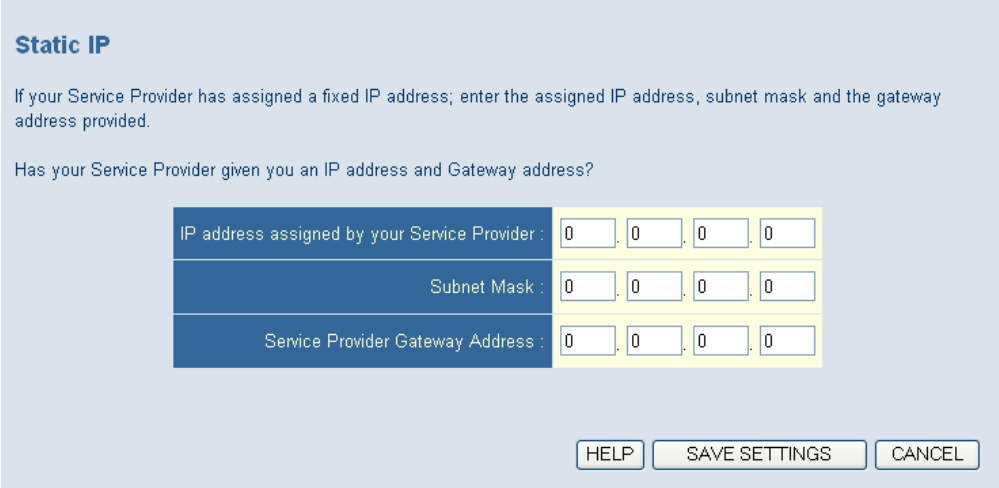
Auto-connect: This option will re-connect when you attempt to access the Internet.

Keep session: This option keeps your PPTP online by having the Barricade continually check your internet connection. If you are disconnected – it will automatically reconnect you.

Need some more help?
If you are having problems getting online with your PPPoE connection type, please refer to **Appendix B | Troubleshooting Internet Connections**.

8.2.4 | Static IP Address

If your ISP has provided you with permanent IP Information, the you will use this option.



IP Address: This is the IP Address assigned to you from your ISP.

Subnet Mask: This is the Subnet Mask assigned to you from your ISP.

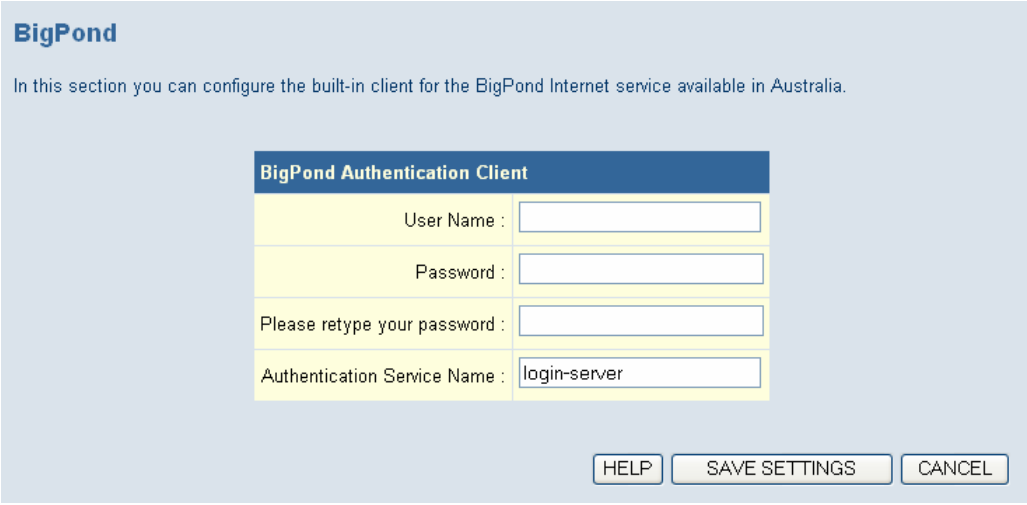
Gateway Address: This is the Gateway IP Address assigned to you from your ISP.

Note: If you don't have this information, please contact your ISP to obtain it.

CAN'T GET ONLINE?
If you are having problems getting online with your Static IP connection type, please refer to **Appendix B | Troubleshooting Internet Connections**.

8.2.5 | BigPond®

Use this section to configure the built-in client.

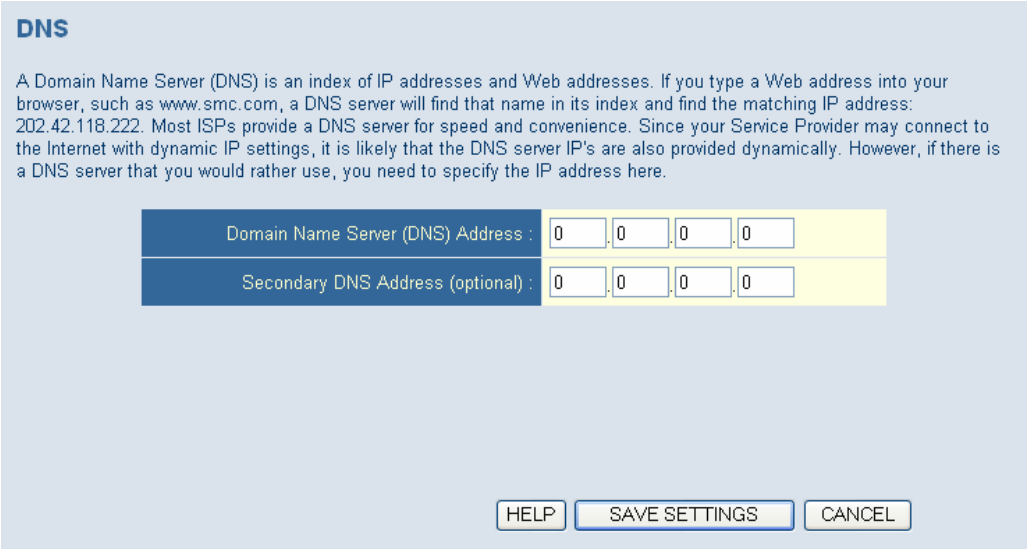


User Name and Password: Enter in the username and password provided by the ISP.

Authentication Service Name: login-server is the default setting for this – unless required by your ISP this will not need to be changed.

8.2.6 | DNS

The Domain Name Services is how the Internet translates domain or website names into Internet addresses (IP Address).



Primary Server: This is the IP Address of the first DNS server will be used first to translate the website name into an IP Address.

Secondary Server: If there is a problem with getting the information from the first server, the Barricade will try this alternative server.

This feature provides 2 configuration options, Static IP DNS Settings and Alternative DNS Settings.

Static IP: If you are using the Static IP Internet connection option, you will need to enter in the DNS Server IP Addresses that your ISP provided you.

Alternative DNS: With any of the other Internet connection types, you can setup the Barricade g to use a custom DNS server that you want to.

8.3 | LAN
From this section, you can configure the Barricade g's LAN interface and DHCP Server settings.

LAN IP - IP Address: This is the IP Address of your Barricade Router.

LAN IP - IP Subnet Mask: Default is 255.255.255.0.

DHCP Server: DHCP is enabled by default, if you have another DHCP server on your network or you don't want to use DHCP, click the [Disabled] option.

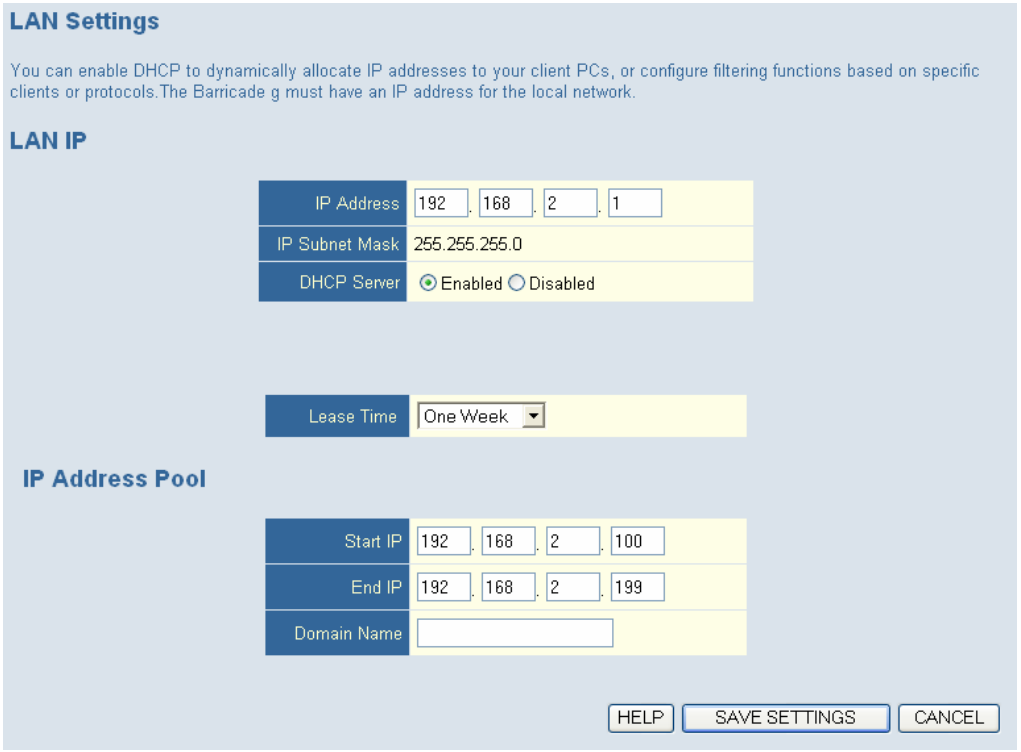
Lease Time: This is the amount of time that a network user will be allowed a connection to the Barricade with there current dynamic IP Address settings. For home networks, this may be set to [Forever], which means there is no time limit on the IP address that is assigned to a client on your network.

IP Address Pool - Start IP: This is the Starting IP Address of the range of IP Addresses that you want to be available for DHCP clients. Default is: 192.168.2.100

IP Address Pool - End IP: This is the ending IP Address of the range of IP Addresses that you want to be available for DHCP clients. Default is: 192.168.2.199

NOTE: Do not include the address of the Barricade g in the DHCP client address pool.

Domain Name: This is the Domain name that will be assigned to the DHCP clients.

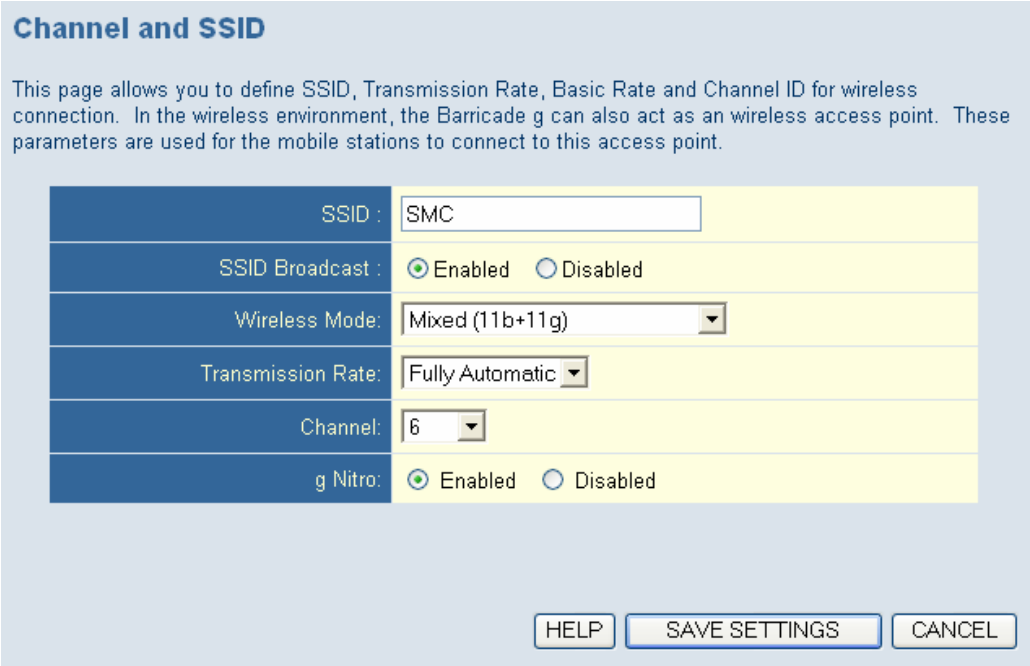


8.4 | WIRELESS

From this section, you can enable or disable the wireless mode, configure wireless settings, and enable or disable the wireless security features like WEP and WPA.

8.4.1 | Wireless Settings (SSID and Channel)

In this section you can configure all the settings for your wireless network.



SSID: This is Name of your wireless network. Default value is [**SMC**]

SSID Broadcast: When enabled your SSID is broadcasted and viewable by other wireless clients. Default value is [Enabled].

WIRELESS SECURITY: To secure your Wireless Network It is recommended that you change the SSID setting and [Disable] the SSID Broadcast feature to hide your wireless network.

Wireless Mode: There are 4 options that you can choose:

- Mixed Mode – in this mode both 802.11b and 802.11g clients can connect to the Barricade g.
- Long Range Mixed Mode – this is a special mode that extends the range of your signal and still allows both 11b and 11g clients to connect.
- 11g Only – in this mode ONLY 802.11g clients can connect to the router.
- 11b Only – in this mode ONLY 802.11b clients can connect to the router.

Transmission Rate: Defines the rate of your wireless signal. It is recommended that you leave this option to [Fully Automatic]

Channel: Select the channel from the list that you want to broadcast your wireless signal on. All devices in your wireless network must be broadcast on the same channel in order to function correctly.

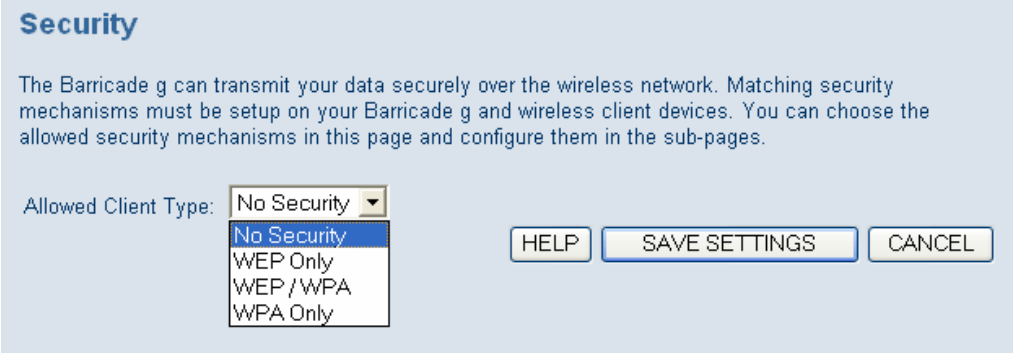
NOTE: If you are experiencing performance issues (i.e wireless distance/throughput) try changing the wireless channel you are using. Doing so may give you improved performance.

g Nitro: Leave this option enabled for improved performance with distance and throughput with your SMC 11g hardware.

8.4.2 | Wireless Security

The Barricade g supports 3 modes of Wireless Security, including WPA, RADIUS, and WEP. These three modes are outlined in the following sections.

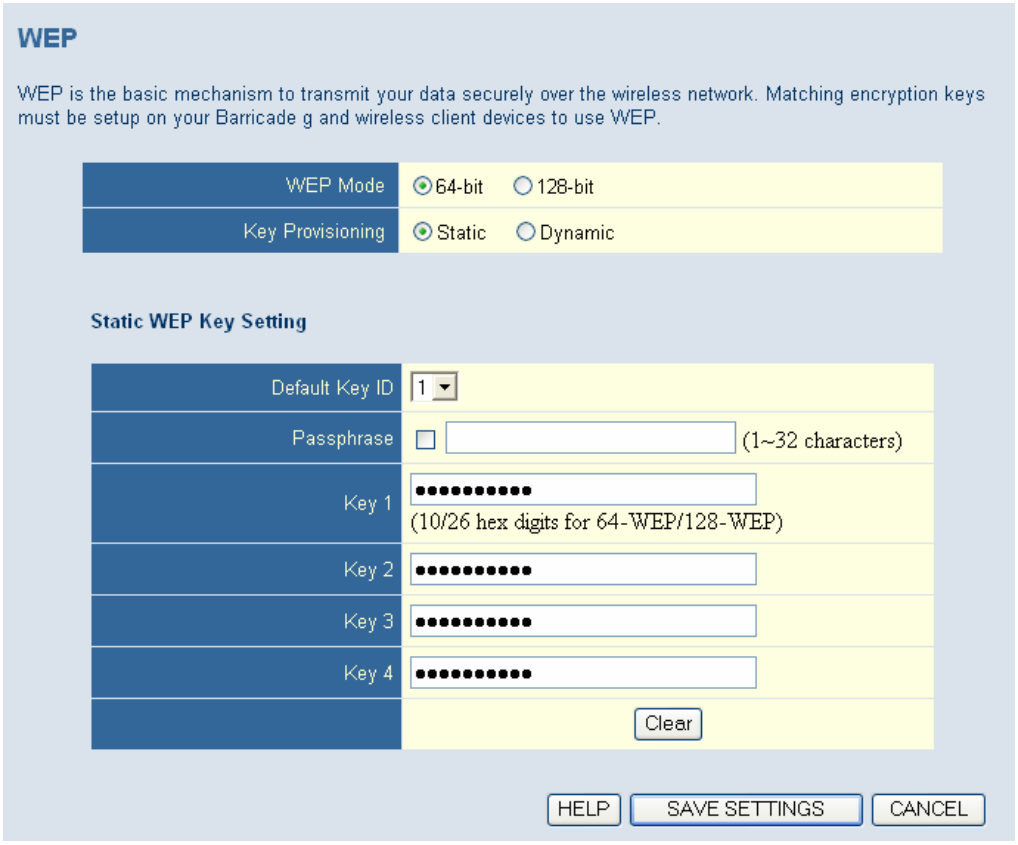
- **WEP** – Wireless Encryption supports 64- and 128-bit and also a pass-phrase feature to auto generate WEP keys.
- **WPA** – Wireless Protected Access, uses Dynamic keys that can be manually entered or auto generated with a pre-shared key (PSK)
- **Radius (802.1x)** – supports authentication through a radius server



NOTE: For ultimate flexibility the Barricade g router can be configured to support both WEP and WPA clients.

8.4.3 | WEP

WEP is a basic encryption method which is not as secure as WPA. However, for most home users, WEP is satisfactory.



WEP Mode: The Barricade g supports 2 WEP modes, 64-bit and 128-bit.

Passphrase: Use this tool to generate a key from a common phrase.

Static WEP Keys: Choose this option if you want to configure the WEP keys in the Barricade g. Depending on if 802.1X authentication is enabled a Radius server may be required.

Dynamic WEP Keys: If you enable the [Dynamic] key option, the Barricade dynamically generates WEP keys when starting up and provides clients with the keys thru EAPOL packets after clients pass 1X authentication. A Radius server is required.

NOTE: When using Dynamic Keys, the 1X authentication should be enabled too, and clients should choose TLS, TTLS, or PEAP to do 1X authentication.

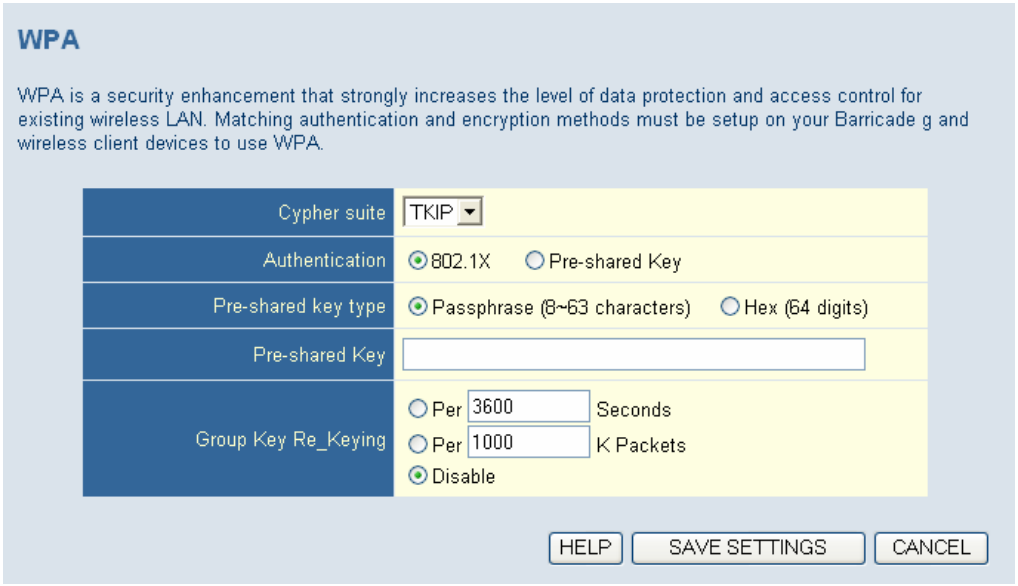
WPA/WEP: If you configure both WEP and WPA (PSK) security options then you will configure your wireless WEP clients to use either WEP key 2, 3, or 4. WEP key 1 cannot be used.

8.4.4 | WPA

Wireless Protected Access or WPA is the latest wireless security enhancement that increases the level of data protection for communicating over wireless networks. There are 2 modes of WPA, PSK (pre-shared key) or Radius (803.1.x).

NOTE: To use WPA you must have a Wireless Client adapter that supports WPA as well as a WPA client.

For Windows XP users, you can download and install a WPA update from the Microsoft site.



Cypher Suite: Only TKIP is supported

802.1X Authentication: Requires a Radius server is configured in the 802.1x section.

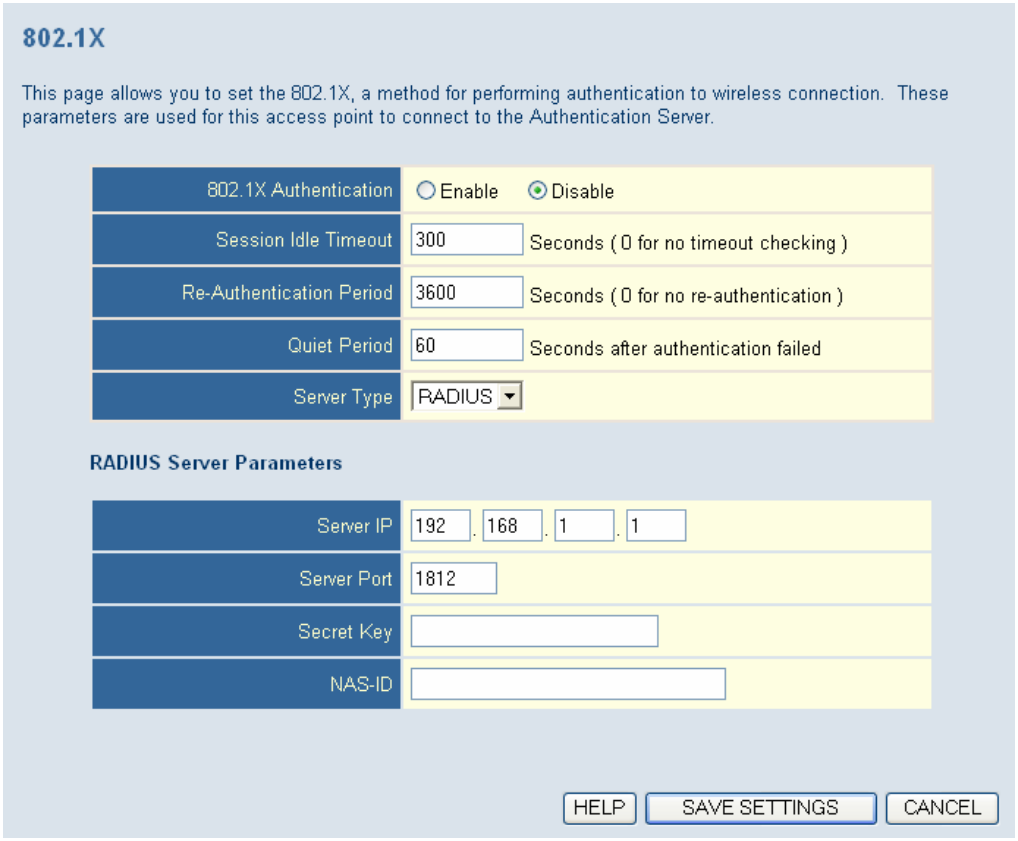
Pre-shared Key (PSK) Authentication: Uses a pre-shared key to do authentication. No Radius server is required. The pre-shared key can be generated using with passphrase style or manually defined with 64 HEX characters.

Group Key Re-keying: This in the interval time period of renewing broadcast/multicast the dynamic WPA key to each wireless client on your network.

NOTE: When both WEP and WPA clients are allowed, the Group Key Re-keying function will automatically be disabled.

8.4.5 | Radius (802.1x)

WEP or WPA can be used in coordination with a RADIUS server is connected to the Router or on the same Network.



Session Idle Timeout: This is the time (in seconds) that a session will be inactive before terminating. Set 0 if you do not want the session to timeout.

Re-Authentication Period: The time interval required for the client to re-authenticate again. For example, if you set this to 30 seconds, the client will have to re-authenticate every 30 seconds.

Quiet Period: This value is the time (in seconds) the Barricade will wait between failed authentications.

Server IP: Set the LAN IP address of your Radius Server.

Server Port: Set the connection port that is configured on the Radius server.

Secret Key: This is the 802.1X secret key shared between the Barricade g and the Radius server.

NAS-ID: The NAS ID is an alphanumeric string or an IP address that the RADIUS server uses to identify packets from the server. The value you enter here will be sent in the NAS-Identifier (32) attribute in all Access-Request packets sent to this RADIUS server. By default, the NAS ID is the name of the server.

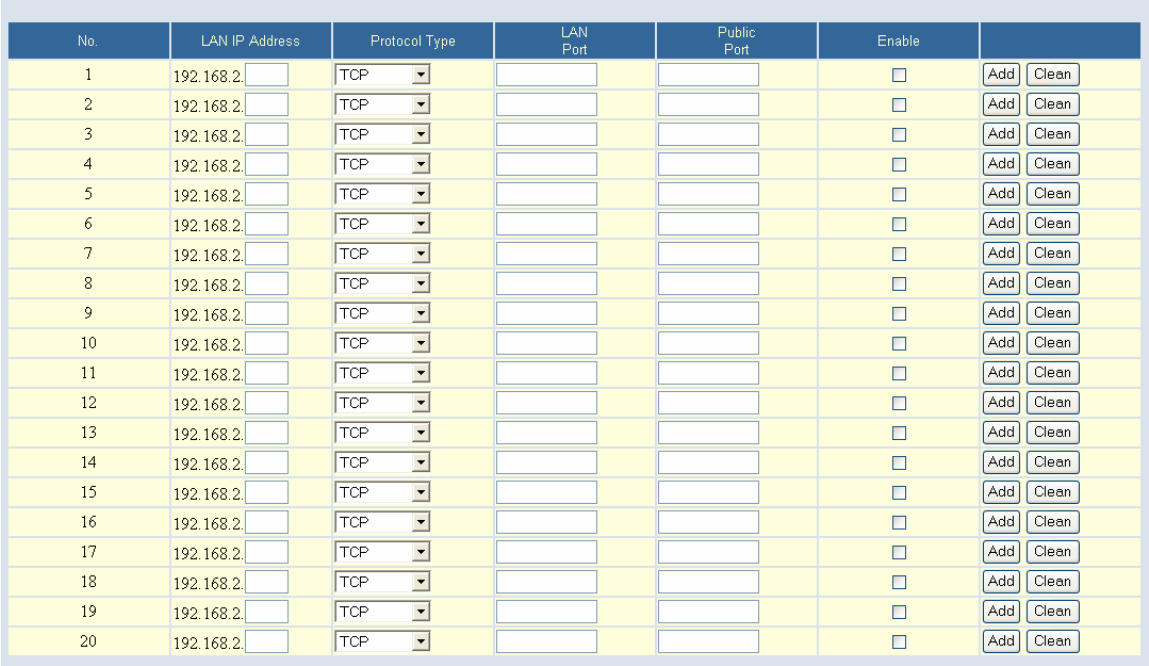
8.5 | NAT

From this section, you can configure the Virtual Server and Special Application features that provide control over the port openings in the router's firewall. This section can be used to support several Internet based applications such as online games.

8.5.1 | Virtual Server

The Virtual Server section allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (i.e. videoconferencing or online gaming.)

NOTE: Some Internet applications may not require any forwarding.



No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.2.	TCP			☐	Add Clean
2	192.168.2.	TCP			☐	Add Clean
3	192.168.2.	TCP			☐	Add Clean
4	192.168.2.	TCP			☐	Add Clean
5	192.168.2.	TCP			☐	Add Clean
6	192.168.2.	TCP			☐	Add Clean
7	192.168.2.	TCP			☐	Add Clean
8	192.168.2.	TCP			☐	Add Clean
9	192.168.2.	TCP			☐	Add Clean
10	192.168.2.	TCP			☐	Add Clean
11	192.168.2.	TCP			☐	Add Clean
12	192.168.2.	TCP			☐	Add Clean
13	192.168.2.	TCP			☐	Add Clean
14	192.168.2.	TCP			☐	Add Clean
15	192.168.2.	TCP			☐	Add Clean
16	192.168.2.	TCP			☐	Add Clean
17	192.168.2.	TCP			☐	Add Clean
18	192.168.2.	TCP			☐	Add Clean
19	192.168.2.	TCP			☐	Add Clean
20	192.168.2.	TCP			☐	Add Clean

To open or forward a port follow the steps outlined below:

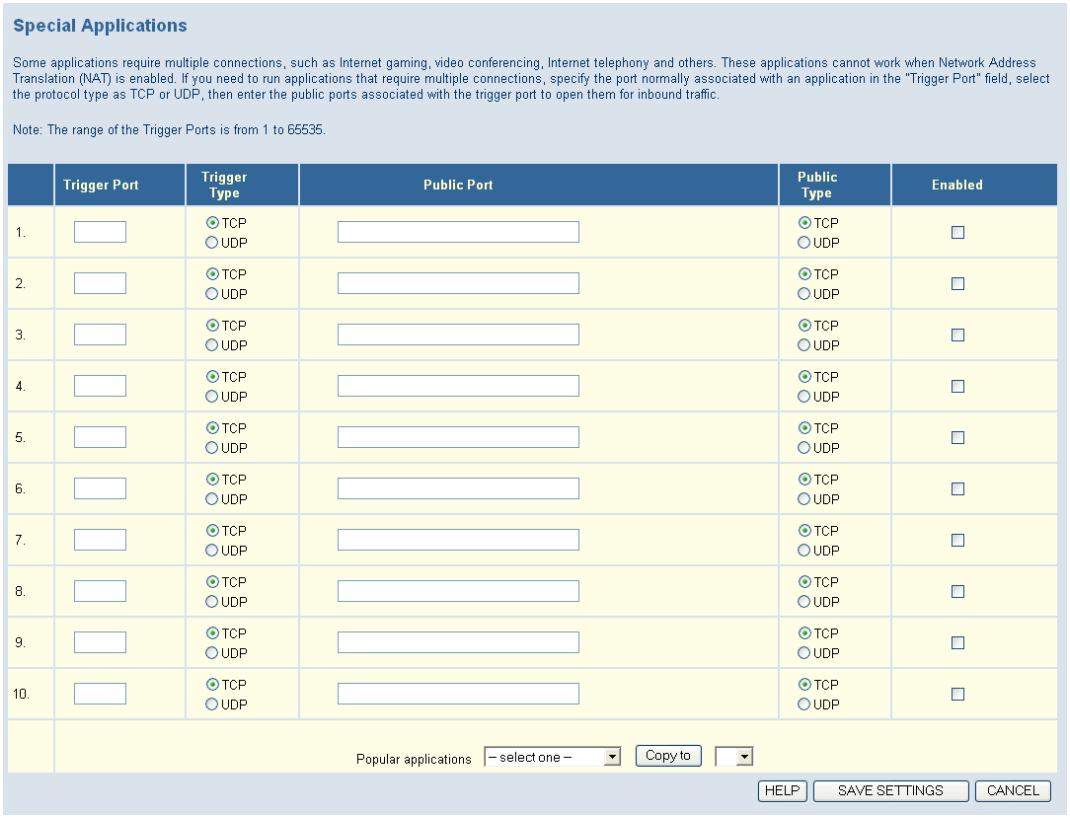
1. Enter in the IP Address of the PC on your network that you want all of this data/traffic directed to.
2. Select the Protocol Type. This can be TCP, UDP, or Both types of data.
3. Enter in the LAN or Private port; this is the internal port that you want this traffic directed to.
4. Enter in the WAN or Public Port; this is the external port the traffic will be coming in from the WAN side.
5. Check the Enable option, and click the [Add] button.

NOTE: If you want to temporally disable a virtual server rule, simply uncheck the Enable option and click the [Add] button. If you want to remove the virtual server rule, then click the [Clean] button.

Need Port Info?
For a list of the ports required by some of the popular online games and other applications please refer to **Appendix C | SMC Port List for Games and Applications.**

8.5.2 | Special Applications

This section allows you to configure dynamic port forwarding rules by using an outgoing trigger port.



Trigger Port: Enter in the outgoing port that will be used to open the public ports

Trigger Type: Choose the protocol type, TCP or UDP traffic.

Public Port: Set the Incoming Range of ports that will be opened by the outgoing trigger port data. The maximum range that you can use for all NAT ports is 0 to 65535.

Public Type: Choose the protocol type, TCP or UDP traffic.

Enabled: You can enable or disable these rules as needed.

NOTE: For security, if you are not using a Special Applications rule, it is recommended that you disable the rule until needed.

Need Port Info?
For a list of the ports required by some of the popular online games and other applications please refer to **Appendix C | SMC Port List for Games and Applications.**

8.6 | Firewall
The firewall does not significantly affect system performance, so we advise enabling it to protect your network users.

To enable the Stateful Packet Inspection (SPI) firewall, click on the [FIREWALL] link in the side navigation bar, select the [Enable] option and click the [SAVE SETTINGS] button.

Once the Barricade g Firewall is enabled, you will have be able to access several other features, including:

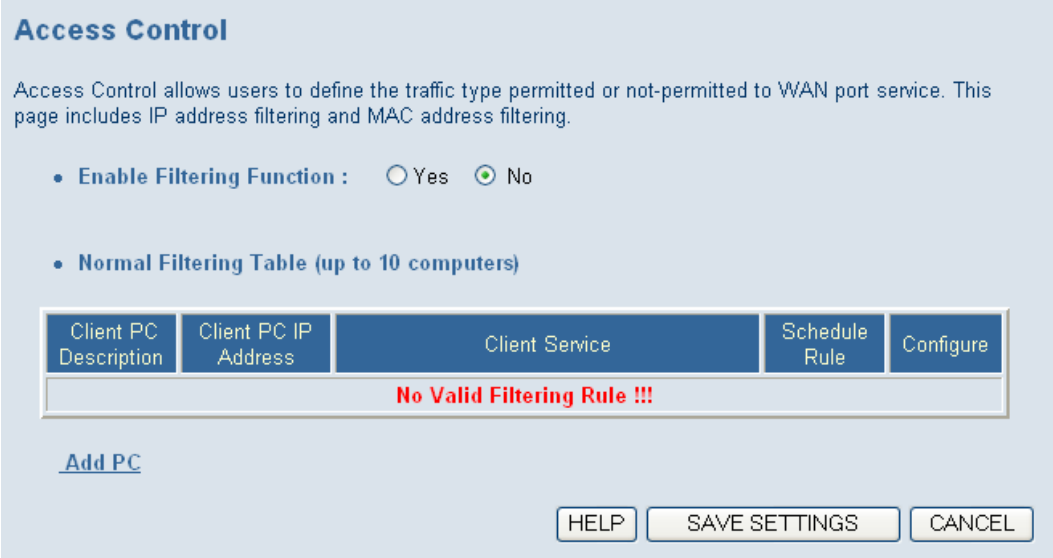
- Access Control
- MAC Filter
- URL Blocking
- Schedule Rule
- Intrusion Detection
- DMZ

The following sections outline each of these options.

8.6.1 | Access Control

Using this option allows you to specify different privileges for the client PCs. This is an excellent tool to control a child's access to specific content and/or general internet access for a specific time and/or date.

To setup an Access Control Rule: Click on [Click Add PC] link to access the [Access Control Add PC] configuration page.



Rule Description: Set a Rule Description so you know what this rule applies to. Ex. Jon's Internet Access.

Client PC IP Address: Set the IP Address Range of the LAN PCs that you want to apply this rule to.

NOTE: If you only want to apply the rule to one PC, just enter in the IP address twice. For example, if you want to setup a rule for LAN IP: 192.168.2.100 – your IP range would be 100-100.

Client PC Service: This is a section of pre-defined services. To block one of these services simply check the [Blocking] option next to the service name.

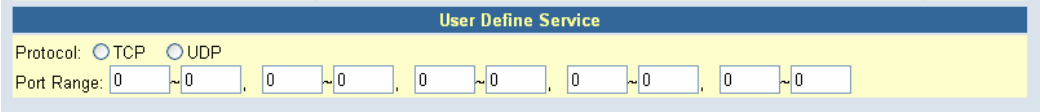
For URL/Website blocking you will need to enter in the Websites and Keywords that you want to block in the URL Blocking section.

Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	☐
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☐
NetMeeting	H.323, TCP Port 1720	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐
VPN-PPTP	TCP Port 1723	☐
VPN-L2TP	UDP Port 1701	☐
TCP	All TCP Port	☐
UDP	All UDP Port	☐

User Define Service: In this section you can define custom services that you want to block. To configure, select the Protocol you want to block and then select the range of ports.

NOTE: This section is useful for blocking new applications, such as Peer-2-Peer file sharing applications that don't use ports defined in the other section.



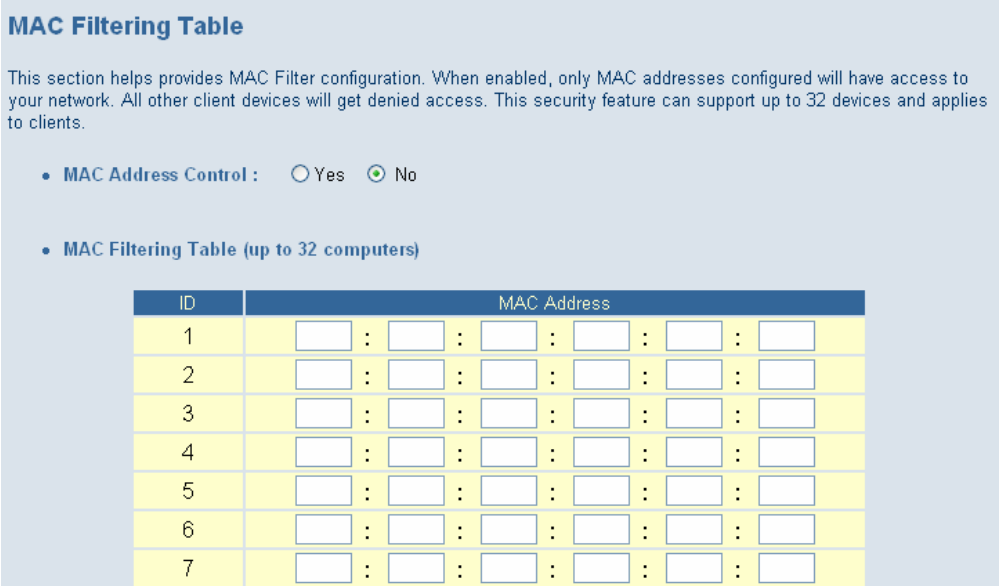
Scheduling Rule: From this option you can select the schedule that you want this Access Control Rule to be active. By default it is set to [Always Blocking].

NOTE: If you want to configure a specific time/date for this Rule to be active you will need to configure the [Schedule Rule] configuration page. When you set-up a custom schedule rule, it will be listed in the drop-down menu as an option.

8.6.2 | MAC Filtering

The MAC Filtering feature of the Barricade allows you to control access to your network based on the MAC (Media Access Control) Address of the client machine. This ID is unique to each network adapter.

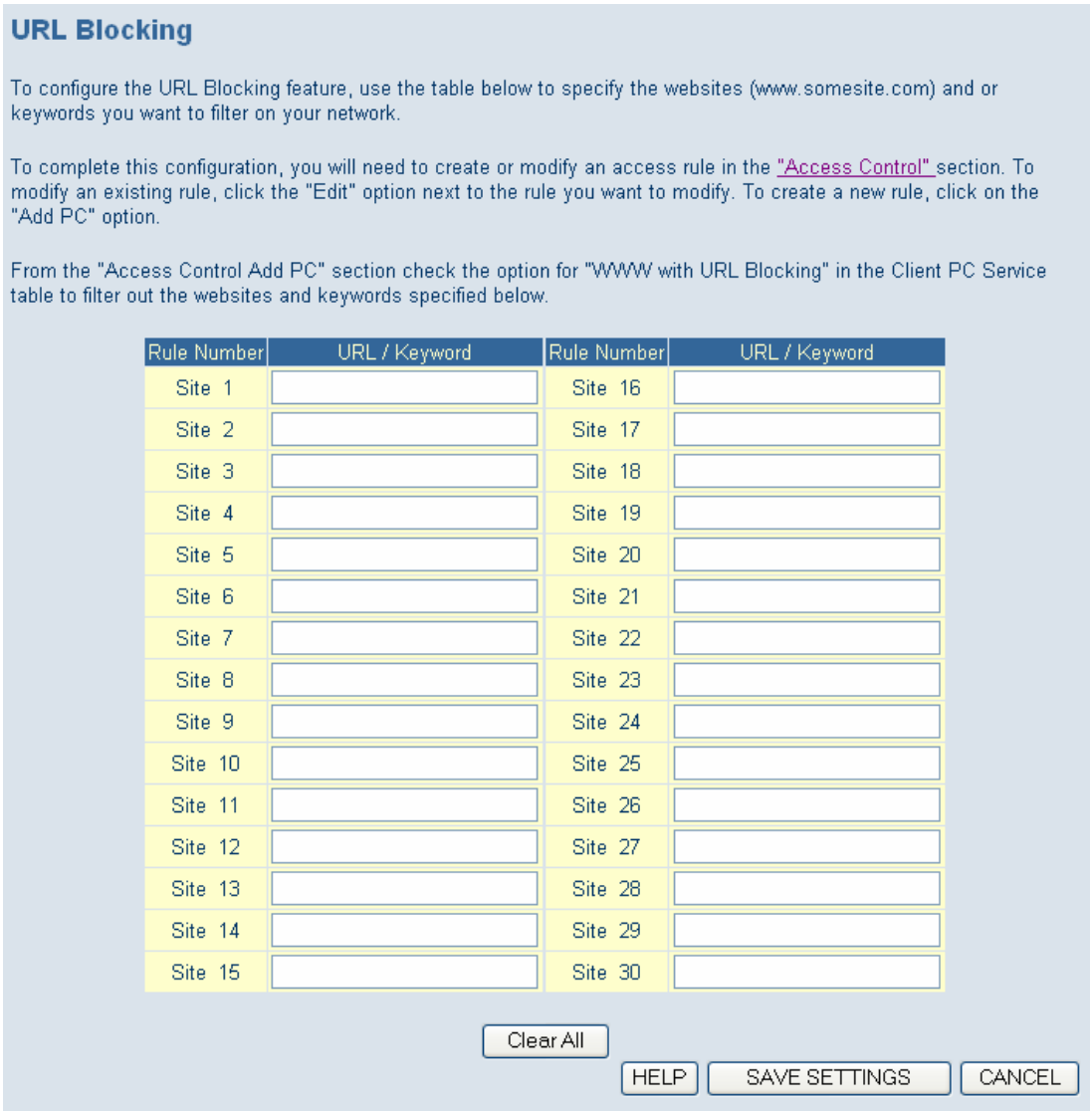
When this option is [ENABLED], each MAC Address listed in the table will be allowed to access the network and Internet.



NOTE: You must have at least ONE MAC address listed in this table when the feature is enabled.

8.6.3 | URL Blocking

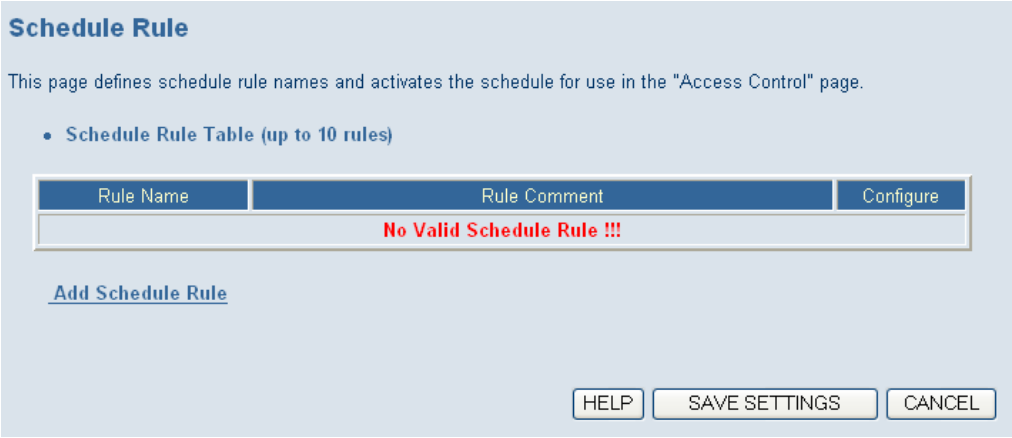
The URL Blocking feature of the Barricade limits access to website domains (i.e. www.somesite.com) or by using keywords which will block any websites that have that keyword in the URL. This feature is an ideal way to protect your family members from questionable content on the Internet



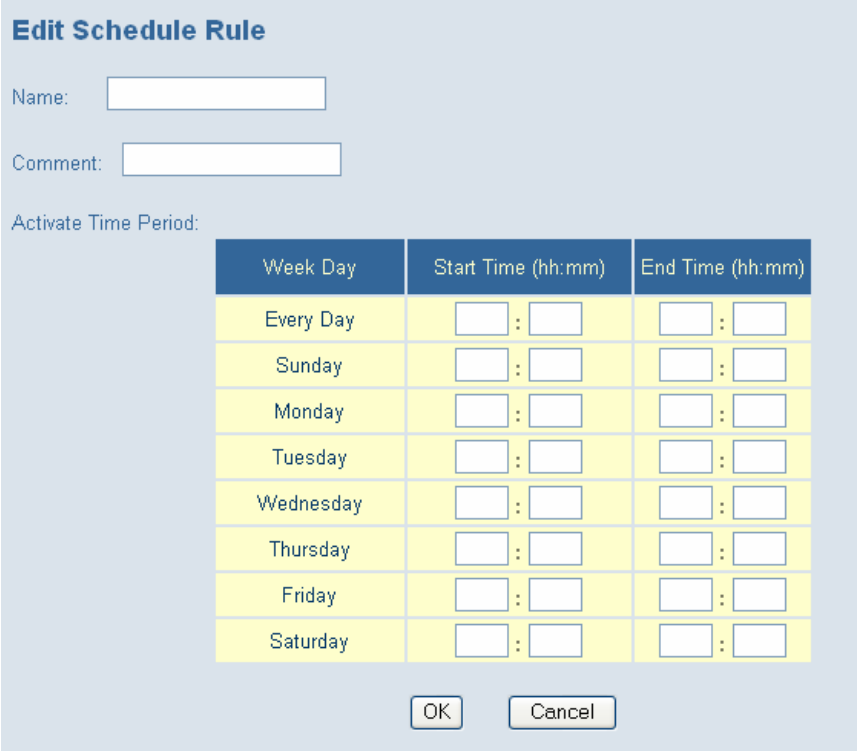
NOTE: This blocking feature applies to the words and URLs typed in the Address Bar of your Browser.

8.6.4 | Schedule Rule

This section allows you to configure up to 10 schedule rules that can be used with the Access Control Rule feature.



To create a Schedule Rule, click the [Add Schedule Rule] link to access the [Edit Schedule Rule] configuration page.



Name: The Name of your schedule rule, for example "block kids internet"

Comment: A comment about the schedule rule, for example the time period "7AM – 7PM"

Activate Time Period: This is the span of time that you want the Access Control rule active and also the day of the week that you want it active.

NOTE: The Start and End Time are set in military time (1705 = 5:05PM)

8.6.5 | Intrusion Detection

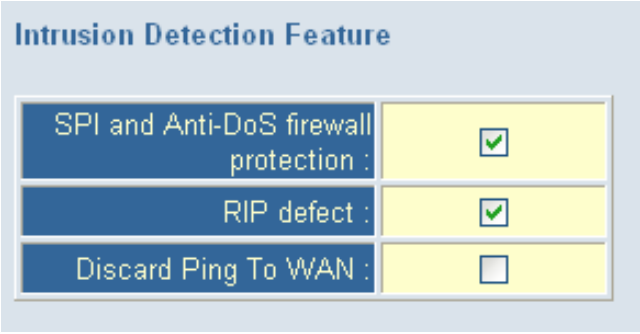
The Barricade g inspects packets at the application layer, and maintains TCP and UDP session information, including timeouts and the number of active sessions. The Barricade g also provides the ability to detect and prevent certain types of network attacks such as DoS attacks. Network attacks that deny access to a network device are called denial-of-service (DoS) attacks. Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. The goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

By using inspected information and timeout/threshold criteria, the Barricade g provides following DOS attacks prevention: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attact) , Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attach), UDP port loopback, Snork Attack etc.

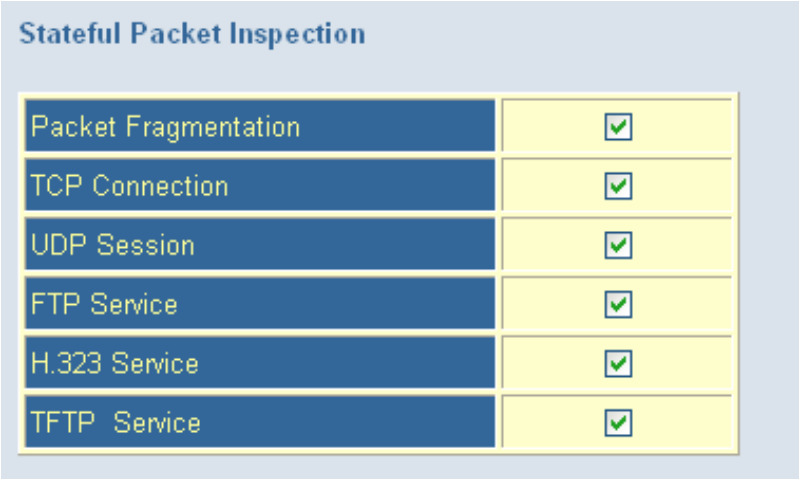
SPI and Anti-DoS firewall protection: Enable/Disable the SPI functions of firewall.

RIP Defect: Enable/Disable the RIP Defect function of firewall.

Discard Ping to WAN: When this feature is enabled, any host on the WAN cannot ping this product. This helps avoid unnecessary attacks from the WAN side because your connection is invisible. It is recommended that you enable this option for security.

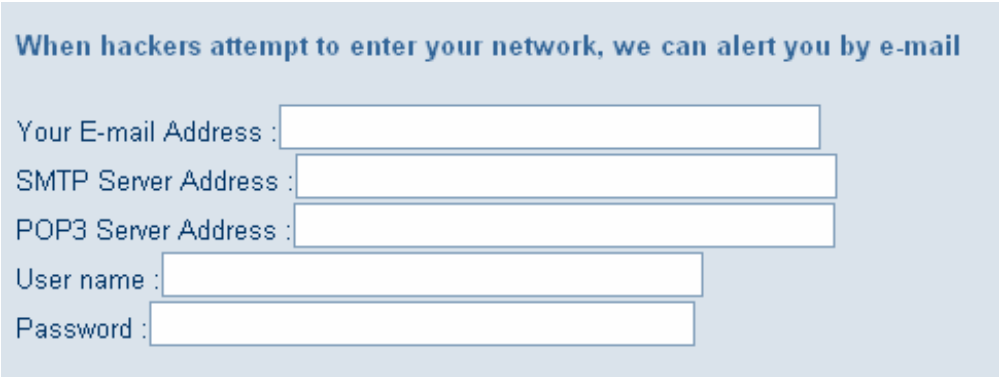


Stateful Packet Inspection (SPI): Use this option to define the type of data you want the SPI firewall to scan.



Email Alert: Configure this option if you want the Barricade to email when hackers attempt to attack your network to a specific email address. You will need to configure your email address, username and password, as well as a SMTP server and POP3 to send the mail through.

NOTE: Some ISPs require that you configure the POP3 server to use there outgoing or SMTP server.

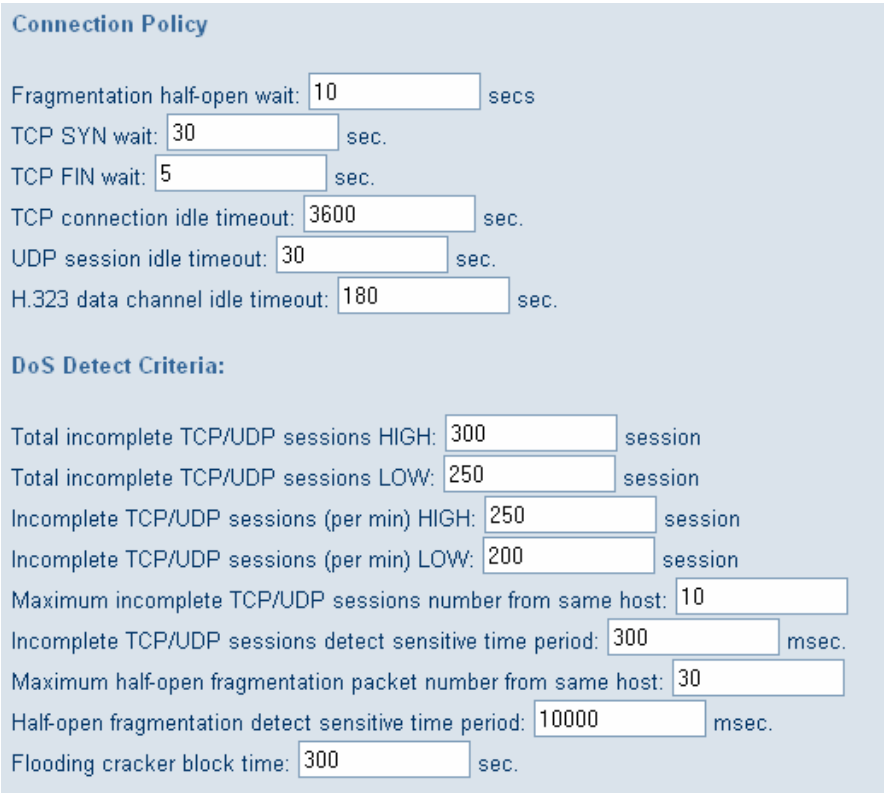


Connection Policy and DoS Detect Criteria: Use both of these sections to tune the Barricade Firewall.

Note: For most users the defaults settings will work fine. If you are having throughput slow downs, then you may want to adjust some of the values under the [DoS Detect Criteria] section:

Change:

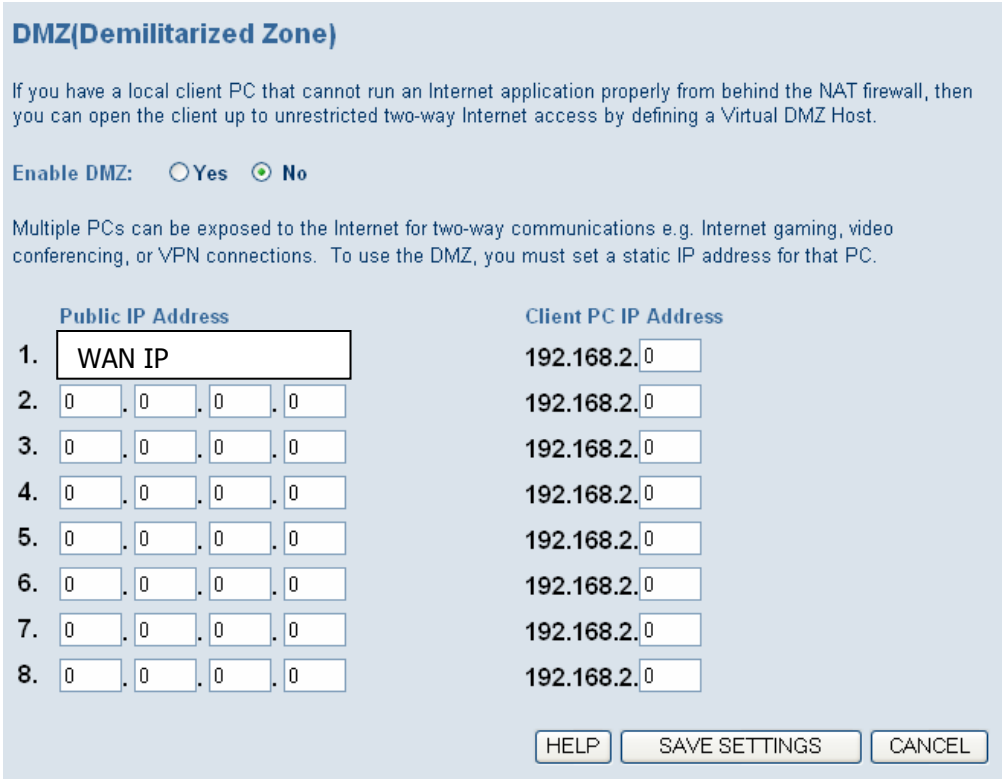
- max incomplete sessions from same host from 10 to 30
- incomplete detect sensitive time period from 300 to 600
- flooding cracker block from 300 to 60



8.6.6 | DMZ (Demilitarized Zone)

If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client PC up to unrestricted two-way Internet access. Enter the LAN IP address of a DMZ host and click "Enable".

NOTE: Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks. Only use this option as a last resort.

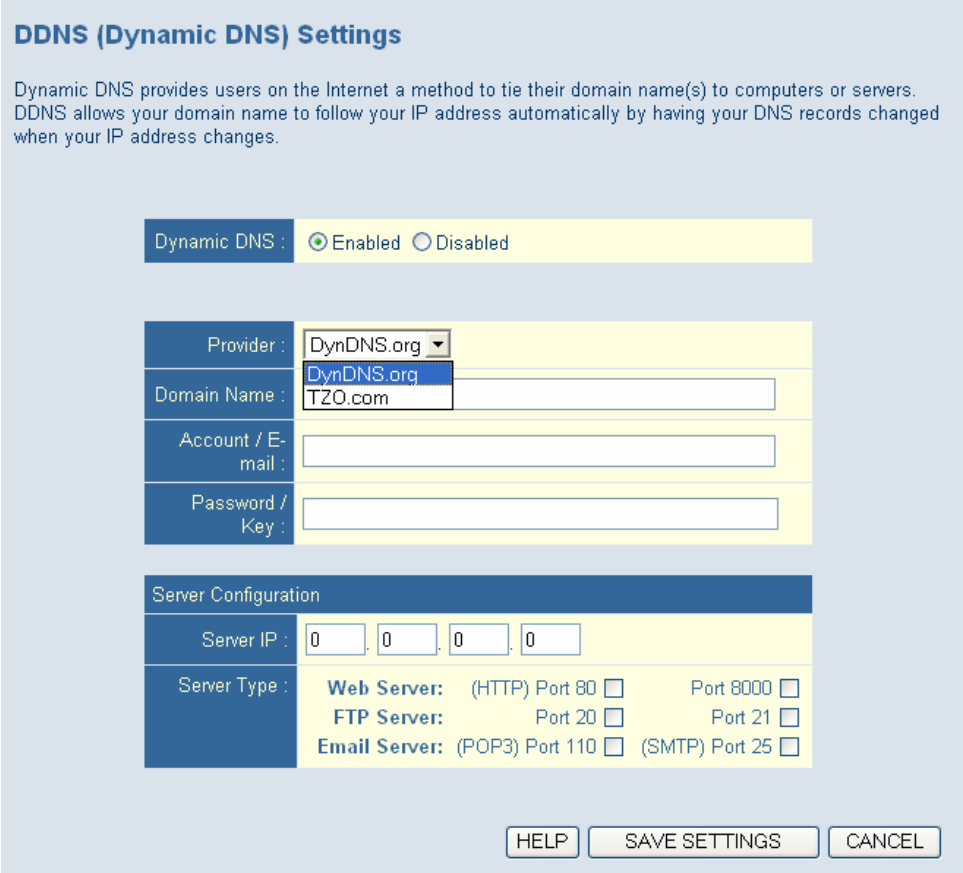


NOTE: To support the 7 other DMZ hosts the IP Address entered must be in the same range as the WAN IP Address.

8.7 | DDNS (Dynamic DNS)
The Barricade has an integrated Dynamic DNS feature that provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

The section also has a "Server Configuration" section that automatically opens the port options checked in the Virtual Server section. Simply enter in the IP Address of your server, such as a web server, and then click on the port option HTTP Port 80 so users can access your server from the WAN connection (Internet).

There are 2 DDNS services supported by this built-in client: DynDNS.org and TZO.com.



Provider: Choose DynDNS.org (www.dyndns.org) or TZO.com (www.tzo.com)

Domain Name: This is the DDNS domain name you have setup with the Provider.

Account / E-mail: TZO.com uses Account information and DynDNS.org uses an E-mail address for [username]

Password / Key: TZO.com uses a auto-generated dynamic key for password and DynDNS.org uses a user-defined password.

Server IP: Enter in the LAN IP Address of your Web Server. (ex. 192.168.2.50)

NOTE: It is recommended that you configure any server on your Network with a static IP addressed.

Server Type: Choose the port traffic that you want routed through the firewall to your server.

8.8 | UPnP

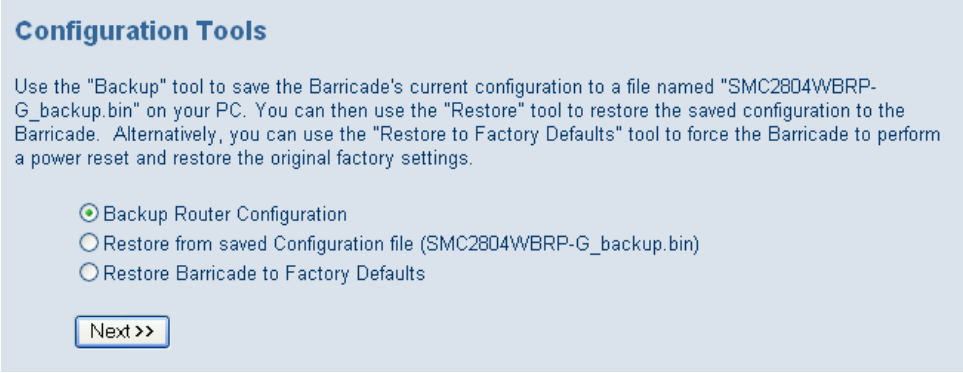
The Barricade supports UPnP (Universal Plug and Play), a networking architecture that provides compatibility amongst networking equipment. This feature allows an UPnP based operating system, like Windows XP to automatically communicate with the Barricade g and open the required services when needed.

NOTE: You will also need to enable this option for non-UPnP based operating systems for Messenger pass-through mode. This will allow Voice, Video, and File Transfer options to work.

8.9 | Tools

Use the "Tools" menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the Barricade.

8.9.1 | Configuration Tools



Backup: Backup saves the Barricade's configuration to a file.

Restore: To restore settings from a saved backup configuration file.

Restore to factory defaults: Restores the Barricade settings back to the factory default settings.

8.9.2 | Firmware Upgrade

This tool permits easy downloading of the latest Firmware. Download the upgrade file from the SMC website (www.smc.com) and save it to your hard drive. Browse for the file and then the click [BEGIN UPGRADE] button.

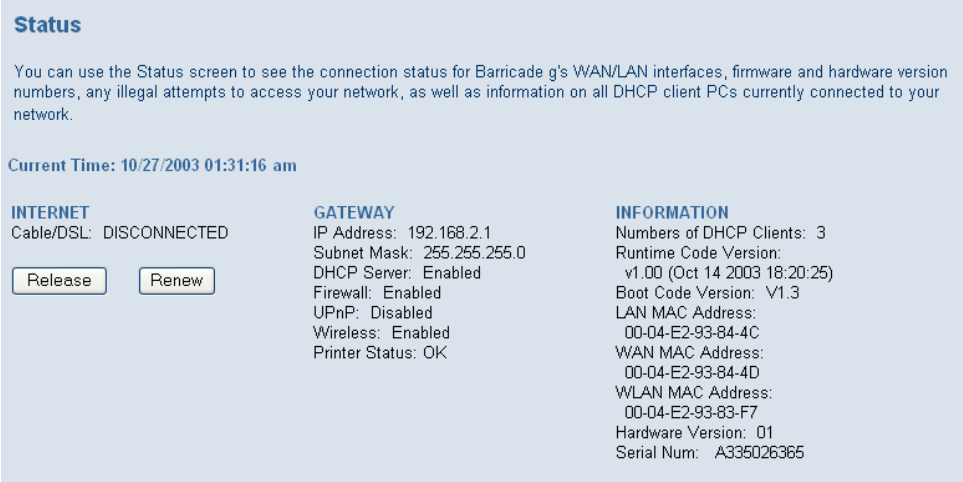
NOTE: When the upgrade process has completed, check the Status page Information section to confirm that the upgrade process was successful.

8.9.3 | Reboot

Click [REBOOT ROUTER] button to reboot the Barricade g. The reset will be complete when the power LED stops blinking and the login page is displayed.

8.10 | Status

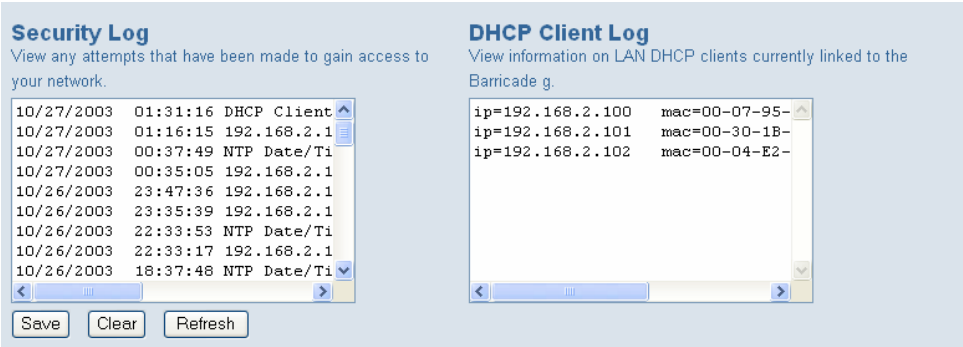
The Status screen displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network.



INTERNET: Displays WAN connection type, status, and if required connection buttons.

GATEWAY: Displays system IP settings, as well as DHCP, UPnP, Wireless, Firewall, and Printer status.

INFORMATION: Displays the number of attached clients, the firmware versions, and the MAC Address for each media interface, as well as the hardware version and serial number.



Security Log: Displays illegal attempts to access your network.

- [Save] Click on this button to save a security log file.
- [Clear] Click on this button to delete the access log.
- [Refresh] Click on this button to refresh the screen.

DHCP Client Log: Displays information on all DHCP clients on your network.

For additional information on the SMC2804WBRP-G, please visit www.smc.com.

CHAPTER 9| Print Server Setup

This chapter will outline the steps to configure the built-in USB print server on the Barricade g Router.

NOTE: This print server will not support multi-function printer devices (ex. Printer, Copier, Fax machine all-in-one)

Windows 98/Me
If you are running Windows 98 or Windows Me then you will need to install the SMC USB Printer Port utility. This utility will re-direct your print jobs to the Barricade g Router.

Installation of SMC USB Printer Port Utility
To install, insert the EZ 3-Click Installation Wizard, and click the [Install Printer Utility] button.

Once you complete the installation you will need to reboot your PC to complete the installation process.

After the reboot, you are ready to re-configure an existing printer or install a new printer.

Configure SMC USB Printer Port with existing Printer

Installing a new Printer with the USB Printer Port Utility

Windows 2000/XP
If you are running Windows 2000 or Windows XP (Home or Professional) you will need to setup the LPR port to redirect printer data to the Barricade g Router built-in USB Print Server.

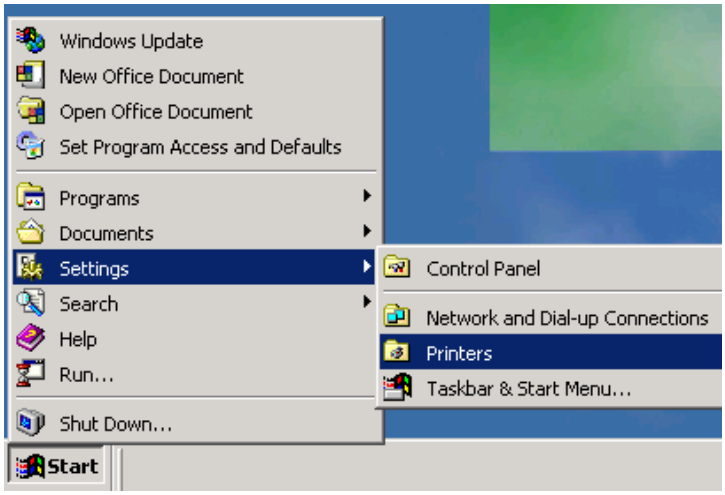
NOTE: The screen shots shown below were done with a Windows 2000 machine, the same steps apply for a Windows XP machine.

Configure LPR port with existing Printer
If you already have the Printer that is connected to the USB Print Server on the Barricade g installed on the PC then you will simply need to re-configure the driver to use the LPR port.

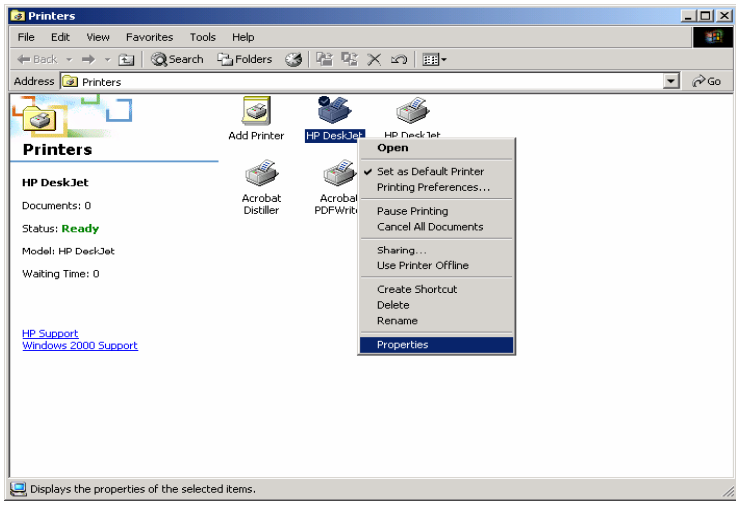
To do this, follow the steps outlined below:

1. Open the [Printers] window – Click [Start] button, choose [Settings], and then click [Printers] option.

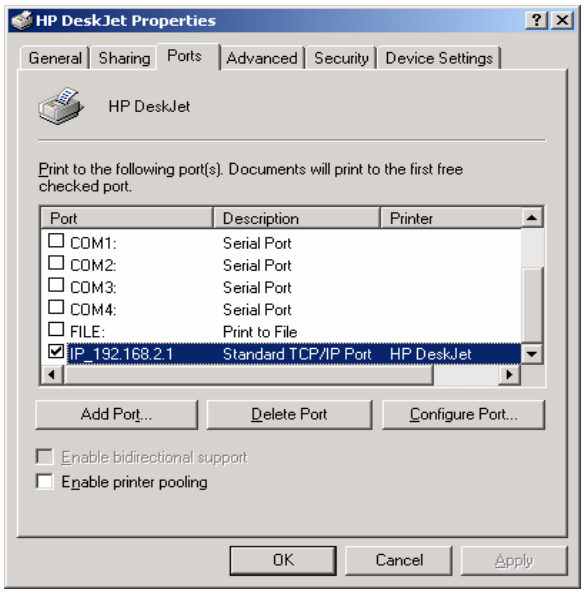
   On Windows XP you will select the [Printers and Faxes] option.



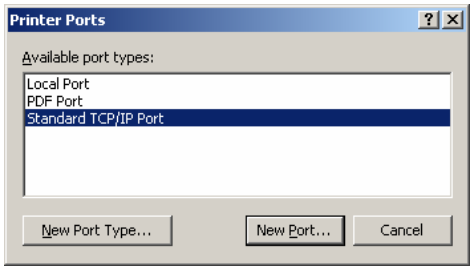
2. In the [Printers] window, locate the icon for your Printer and right-mouse click on it. From the option menu, select the [Properties] options.



3. When the Printer Properties dialog box opens, click the [Ports] tab at the top. In that section, click the [Add Port…] button. This will launch the [Printer Ports] dialog box.

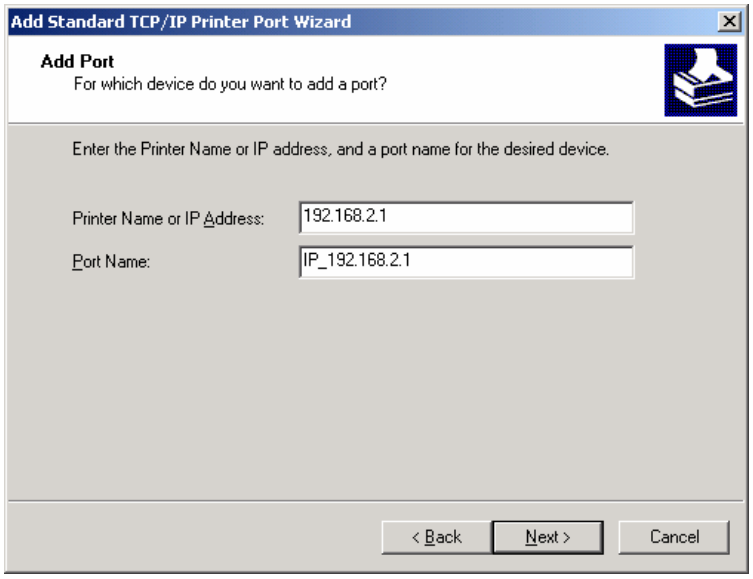


4. In this dialog box, highlight the [Standard TCP/IP Port] option and click the [New Port…] button to launch the [Add Standard TCP/IP Printer Port Wizard]

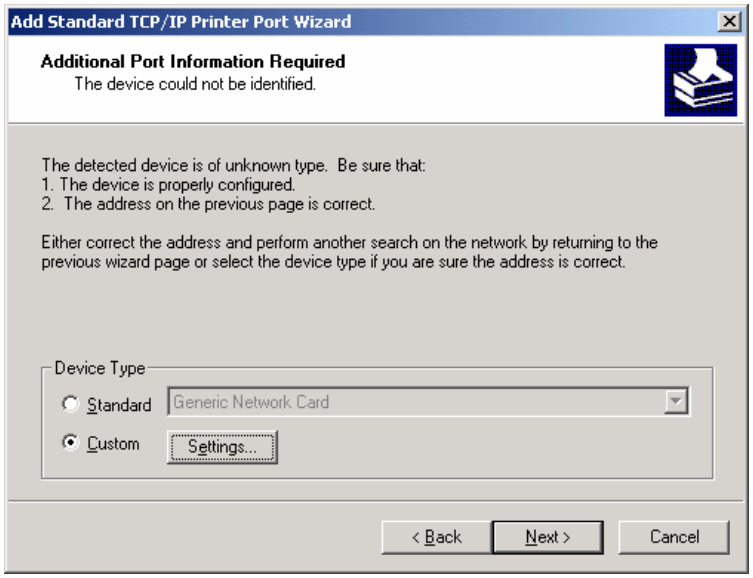


5. Click [Next] button to start the installation.

6. On the [Add Port] step, fill in the IP address of the Barricade g. The default IP is 192.168.2.1. This will automatically fill in the port name – but you can change this can be changed. Click the [Next] button to continue.

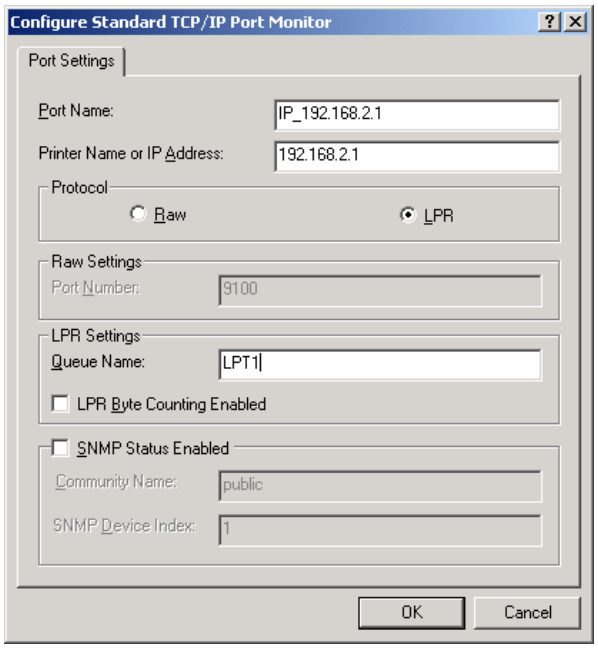


7. When the [Additional Port Information Required] dialog box opens, select the [Custom] option and click the [Settings…] button.



8. At the [Configure Standard TCP/IP Port Monitor] dialog box, select [LPR] for the protocol and enter [LPT1] for the Queue name.

   Click on the [OK] button to save the settings can close this dialog box.

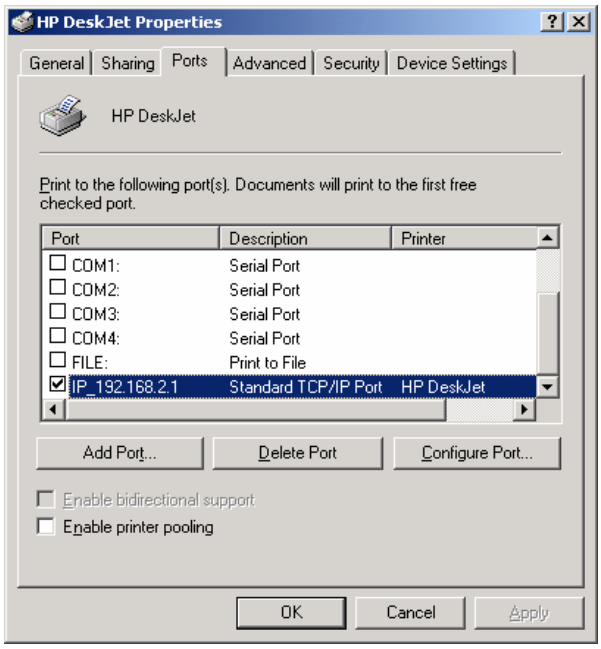


9. This brings you back to the [Additional Port Information Required] screen. Click the [Next] button to continue.

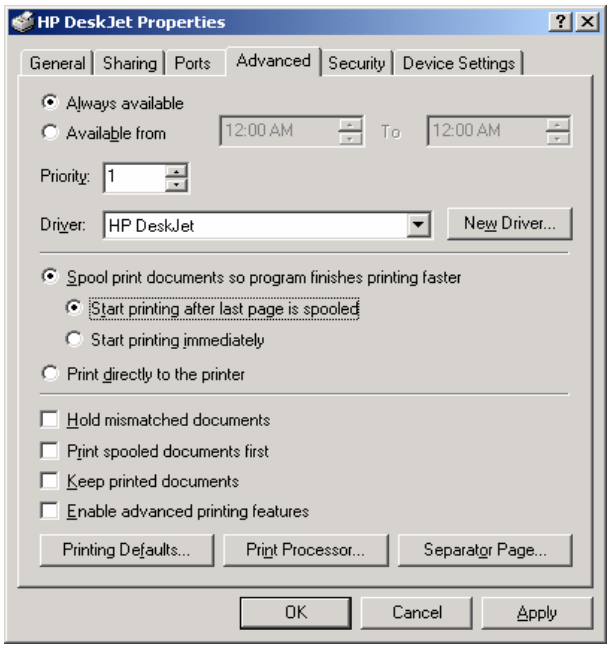
10. You have completed the installation of the LPR printer port click the [Finish] button to complete the process.

11. This brings you back to the [Printer Port] dialog box; click the [Close] button to return to the [Printer Properties] dialog box.

12. On the [Properties] dialog box click the [Ports] tab at the top and then check or confirm that you have the new LPR port selected (ex. IP_192.168.2.1).



13. Click on the [Advanced] tab click the [Spool print documents so program finishes printing faster] and [Start printing after last page is spooled] options.



14. When completed, click the [OK] button, and you are ready to print to the Barricade g with USB Print Server.

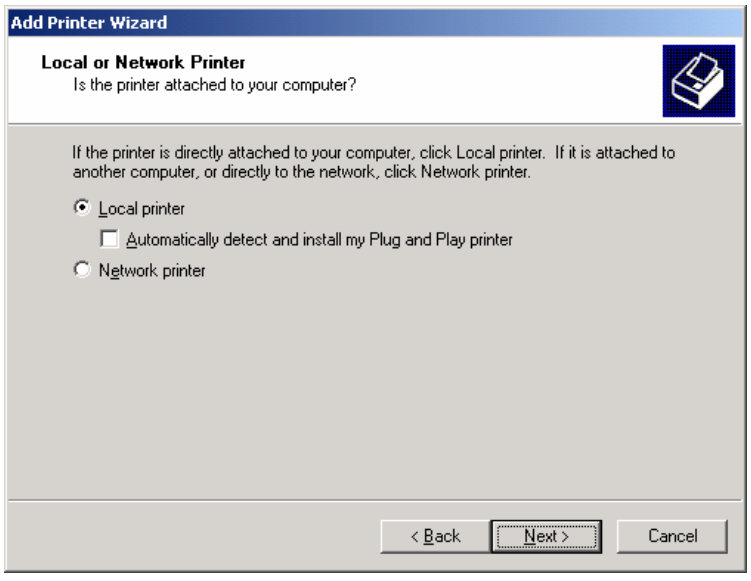
Installing a new Printer with LPR port

1. Open the [Printers] window – Click [Start] button, choose [Settings], and then click [Printers] option.

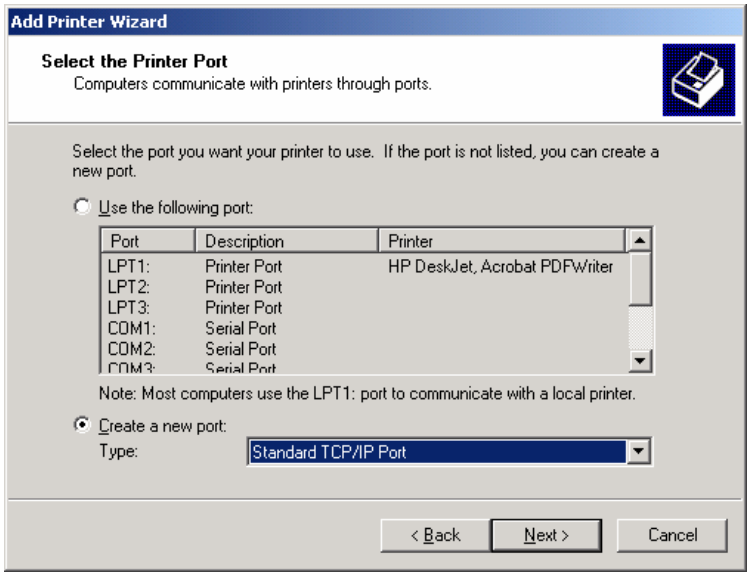
   On Windows XP you will select the [Printers and Faxes] option.

2. In the [Printers] window, click the [Add Printer] icon to launch the [Add Printer Wizard].

3. When the Local or Network Printer window appears, select the [Local printer] option and UNCHECK the [Automatically detect and install my Plug and Play printer] option.

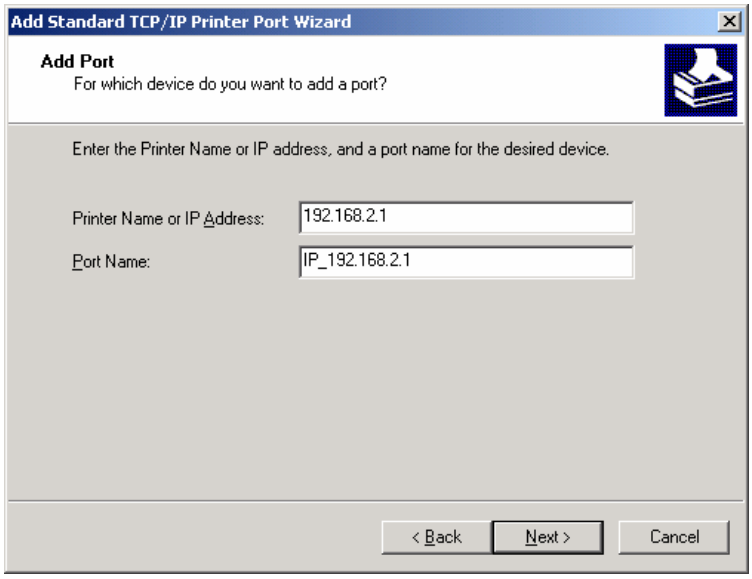


4. On the [Select the Printer Port] step, choose the [Create a new port] option and choose [Standard TCP/IP Port] from the drop-down menu.

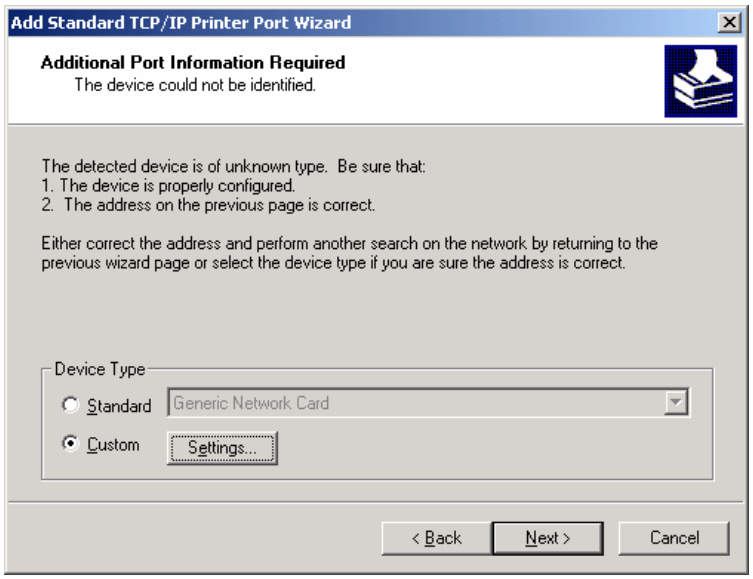


5. This will launch the [Add Standard TCP/IP Printer Port Wizard], click [Next] to start the wizard.

6. On the [Add Port] step, fill in the IP address of the Barricade g. The default IP is 192.168.2.1. This will automatically fill in the port name – but you can change this can be changed.

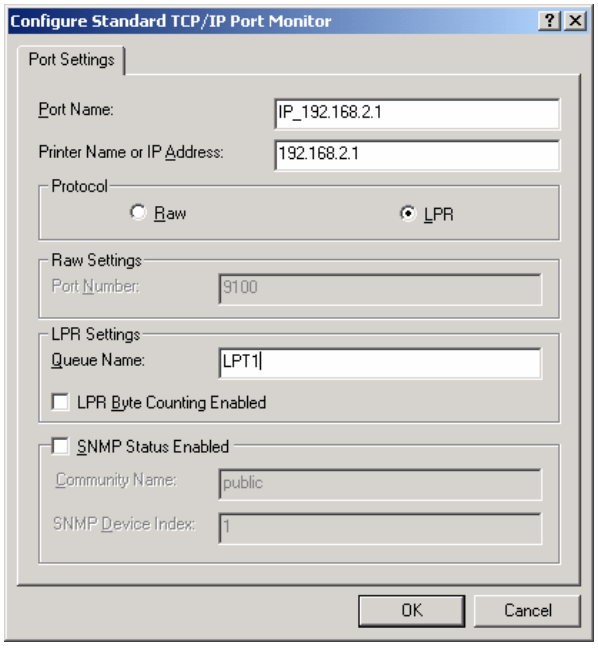


7. When the [Additional Port Information Required] dialog box opens, select the [Custom] option and click the [Settings…] button.



8. At the [Configure Standard TCP/IP Port Monitor] dialog box, select [LPR] for the protocol and enter [LPT1] for the Queue name.

   Click on the [OK] button to save the settings can close this dialog box.

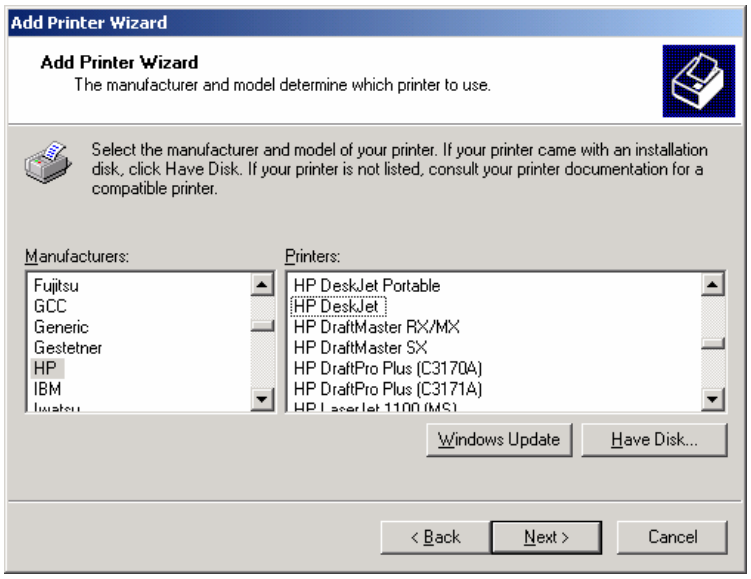


9. This brings you back to the [Additional Port Information Required"] screen, click the [Next] button to continue.

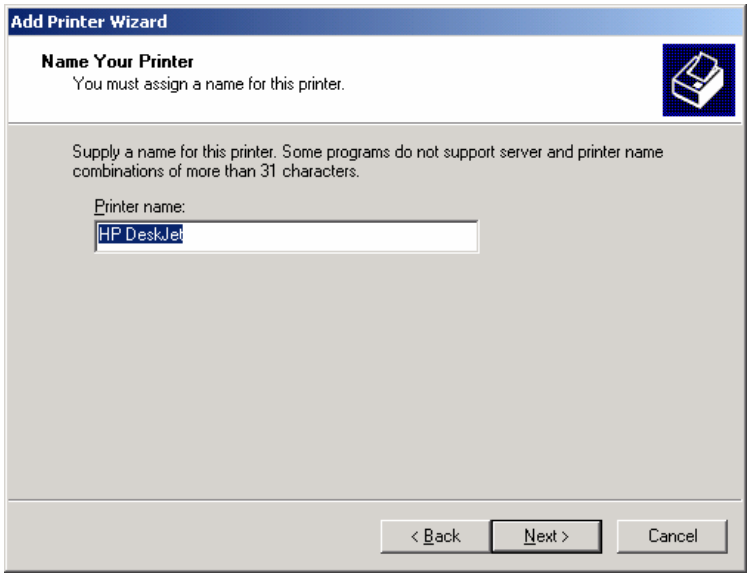
10. Once you have completed the [TCP/IP Printer Port Wizard], click the [Finish] button to complete the process.

11. Next, you will need to install the latest driver for your Printer. Using the [Add Printer Wizard], choose your printers manufacturer and model then click the [Next] button.

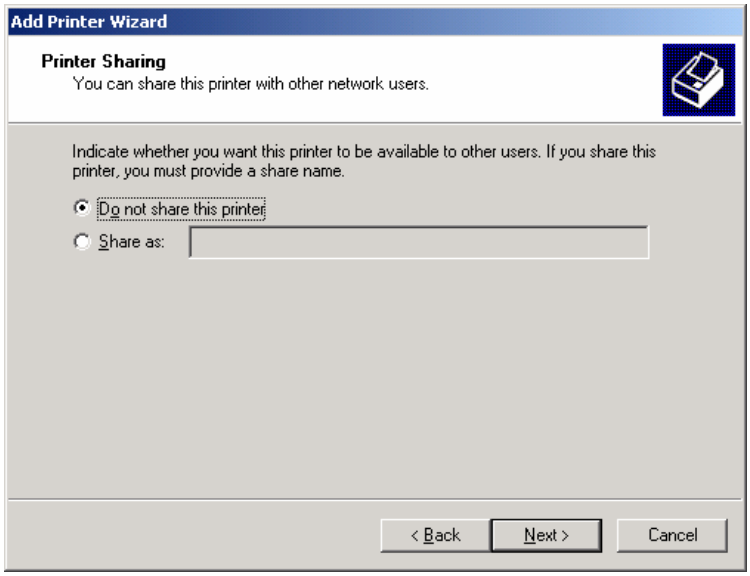
    NOTE: If your printer is not listed, contact your printer manufacture for help on getting it installed.



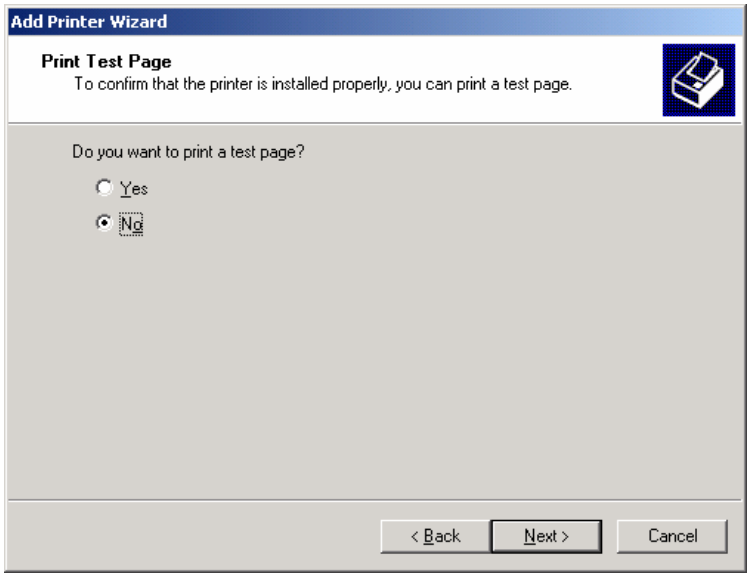
12. On the [Name Your Printer] step, you can enter in the Name of your printer, this can be any value. When completed, click the [Next] button to continue.



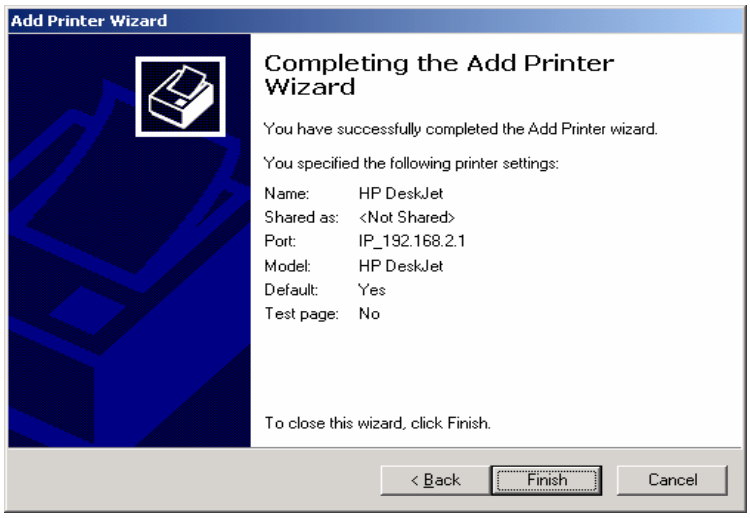
13. At the [Printer Sharing] screen, select the [Do not share this Printer] option and click the [Next] button to continue.



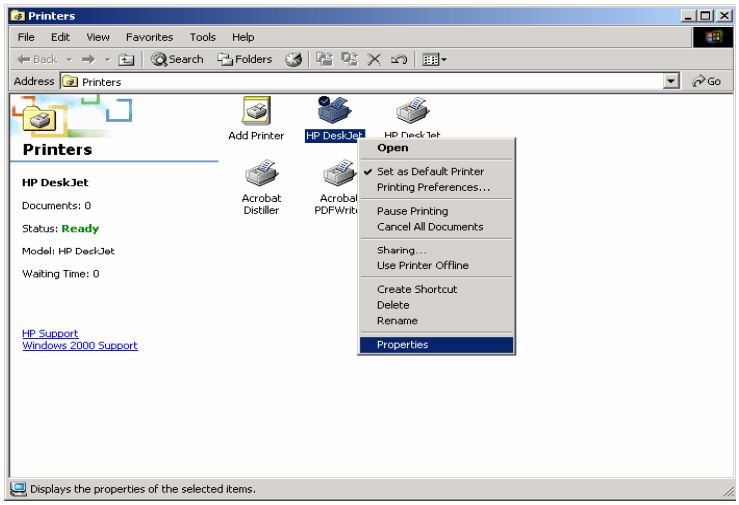
14. At the [Print Test Page] screen, select the [No] option and click the [Next} button to continue.



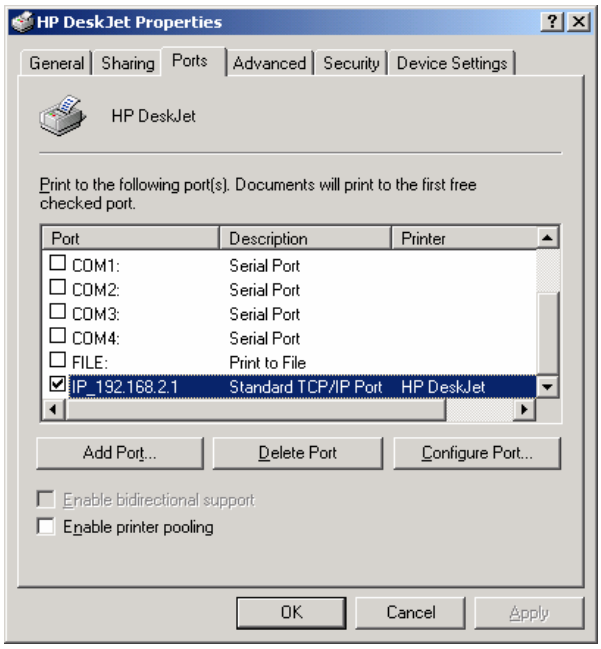
15. At this point you have finished the installation of your printer, click the [Finish] button to save these new settings.



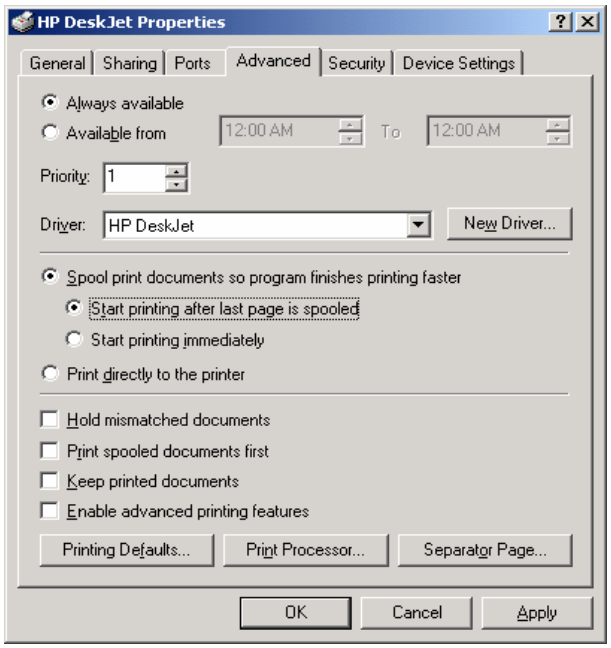
16. When you have finished creating the LPR port and installing the latest printer drivers, then you are ready to configure the printer settings. To access the printers properties, open the printers window and right-mouse click on the new Printer Icon and choose [Properties]



17. On the [Properties] dialog box click the [Ports] tab at the top and then check or confirm that you have the new LPR port selected (ex. IP_192.168.2.1).



18. Click on the [Advanced] tab click the [Spool print documents so program finishes printing faster] and [Start printing after last page is spooled] options.



19. When completed, click the [OK] button, and you are ready to print to the Barricade g with USB Print Server.

APPENDIX A | Troubleshooting

The information outlined in this section describes some useful steps for getting your computer and Barricade router online.

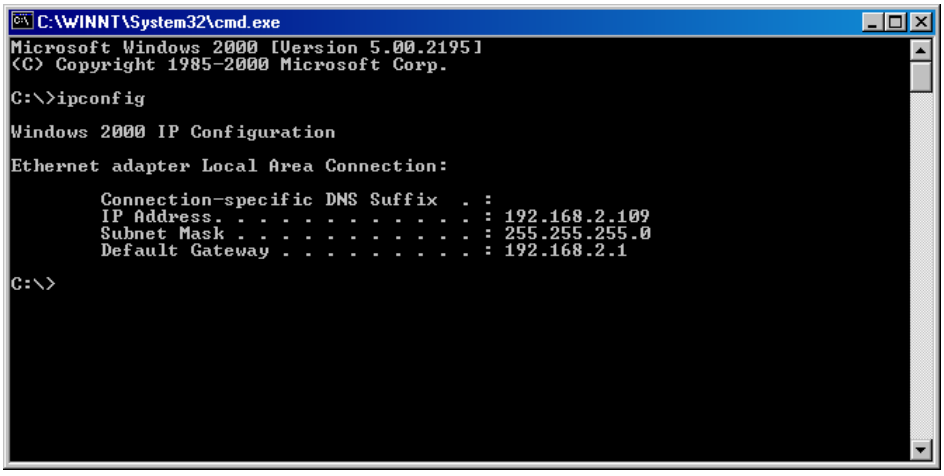
A.1 | Verify you are connected to the Barricade Router

If you are unable to access the Barricade's web-based administration pages, then you may not be properly connected or configured. The screen shots in this section were taken on a Windows 2000 machine, but the same steps will apply to Windows 95/98/Me/XP.

To determine your TCP/IP configuration status, please follow the steps below:

1. Click [Start] then choose [Run]
2. Type "cmd" or "command" (without the quotes) to open a DOS prompt.
3. In the DOS window, type "ipconfig" and verify the information that is displayed.
4. If you computer is setup for DHCP, then your TCP/IP configuration should be similar to the information displayed:

    - IP Address: 192.168.2.X (x is number between 100 and 199)
    - Subnet: 255.255.255.0
    - Gateway: 192.168.2.1



If you have an IP address that starts with 169.254.XXX.XXX then see section A.2.

If you have another IP address configured, see section A.3.

A.2 | I am getting an IP Address that starts with 169.254.XXX.XXX

If you are getting this IP Address, then you need to check that you are properly connected to the Barricade Router.

Confirm that you have a good link light on the Barricade's port to which this computer is connected. If not, please try another cable.

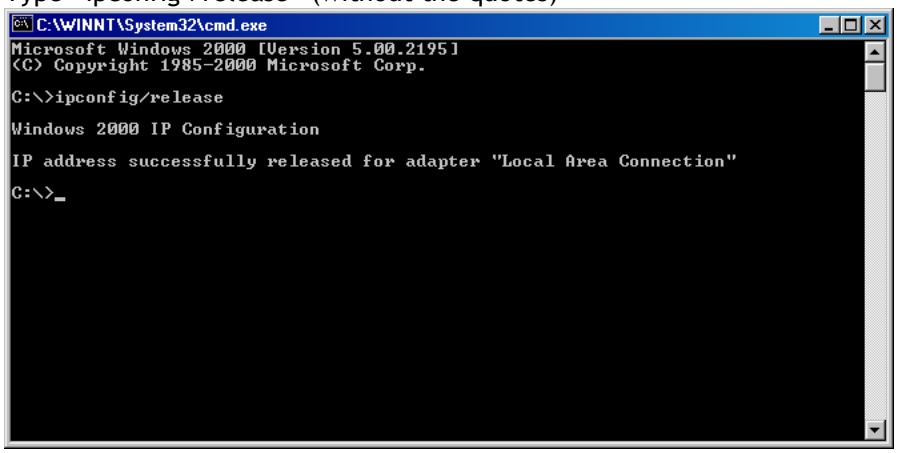
If you have a good link light, please open up a DOS window as described in section A.1 and type "ipconfig /renew" (without the quotes)

If you are still unable to get an IP Address from the Barricade, reinstall your network adapter. Please refer to your adapter manual for instructions.

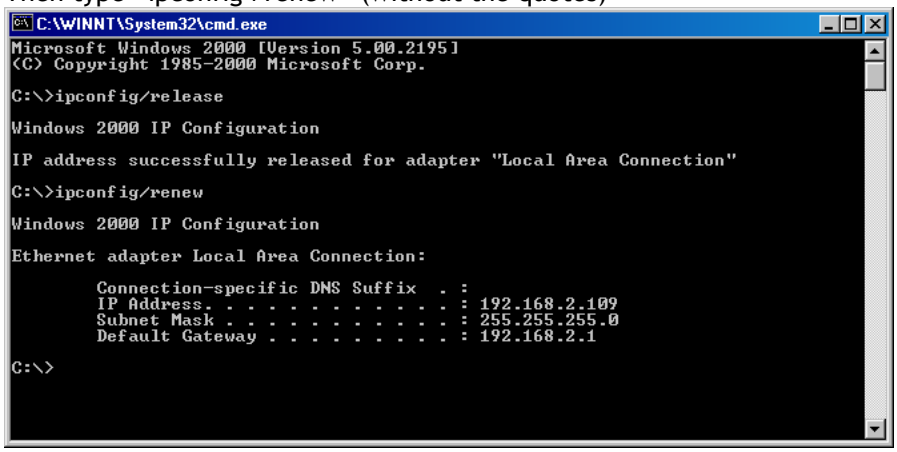
A.3 | I have another IP Address displayed
If you have another IP address listed, then the PC may not be configured for a DHCP connection. Please refer to **Chapter 4 | Configure your Computer** for information.

Once you have confirmed your computer is configured for DHCP, and then please follow the steps below.

1. Open a DOS window as described above.
2. Type "ipconfig /release" (without the quotes)



3. Then type "ipconfig /renew" (without the quotes)



Once you are able to get a valid IP address from the Barricade Router, then you can now access the web-based Administration pages.

If you still are not getting an IP address from the Barricade, please reset the router as outlined in Chapter 2 and follow the steps outlined in this appendix again.

If you still cannot access the router once you have reset it, please contact SMC Technical Support.

A.4 | I can't access my e-mail, web or I am getting corrupted data from the Internet.
The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1454.

For most DSL users, it is strongly recommended to use MTU 1492.

If you are having some difficulties, perform the following steps:

1. To connect to the Barricade g, launch your web browser, and enter http://192.168.2.1 or the IP address of the Barricade in the Address bar.
2. Enter the password, if asked. (The default password is smcadmin.)
3. Click on [WAN] and then select the [PPPoE] option.
4. Look for the MTU option and in the MTU Size field, enter 1492.
5. Click the [SAVE SETTINGS] button to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
1462
1400

APPENDIX B | Troubleshooting Internet Connections

Put information here about specific ISP tricks and how to avoid those basic setup calls.

B.1 | I have a Dynamic IP connection and I can't get online
Most cable companies use a Dynamic IP configuration to provide Internet access. If you have this type of connection, and are unable to get connected, please follow the steps outlined below:

1. Unplug the power from your Cable or DSL modem for 2 mins.
2. Confirm that your Barricade router is configured for a Dynamic IP configuration
3. Plug the power back into your Modem.
4. Wait for your Modem to connect to the network, and then click on the status page of the router to confirm that you are online.

The reason this process works is because certain broadband connections require a MAC address to gain network access. This MAC address can be changed by following the above process to re-set the approved MAC address to the MAC address of the Barricade router.

APPENDIX C | Frequently Asked Questions

Put some of the information that we are finding out with NoHold here – for examples the following information is in the linksys manual.

Does the Router support ICQ send file?
Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get Half-Life: Team Fortress to work with the Router?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

Will the Router function in a Macintosh environment?
Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab.

Make sure that Internet Explorer is set to [Never dial a connection]. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to [Direct connection to the Internet].

How do I get mIRC to work with the Router?
Under the Port Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

How do I reset the Router?
Press the Reset button on the back panel for about ten seconds. This will reset the Router to its default settings.

How do I resolve issues with signal loss?
There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Router and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Router and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment. You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.
WEP is probably enabled on the Router, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

APPENDIX D | SMC Port List for Games and Applications

I need to set up online game hosting or use other Internet applications.
If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

Access the Router's web interface by going to http://192.168.1.1 or the IP address of the Router. Go to the Applications & Gaming => Port Forwarding tab.

Enter any name you want to use for the Customized Application.

Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.4. Check the protocol you will be using, TCP and/or UDP.

Check the protocol you will be using, TCP and/or UDP.

Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Check the Enable option for the port services you want to use. Consider the example below:

Customized	External Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X
Web server	80 to 80	X	X	192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X	X	192.168.1.102	X
POP3 (incoming)	110 to 110	X	X	192.168.1.102	X

Put together a list of all the games/applications ports that we know and confirm work.

COUNTER-STRIKE INFO:

Client
======
TCP 6003:
Outgoing connectivity to this port on remote destinations. Used for chat in the HL browser.

UDP 27011:
Outgoing connectivity to this port on remote destinations. Used for the 'custom game' mod browser.

UDP 27005:
Incoming connectivity to this port (or whatever port the client has changed this to, if not using the default). Used for game traffic (including voice) between client and server.

Server
======
TCP 7002:
Outgoing connectivity to this port on remote destinations. Used for WON auth.

UDP 27010:
Outgoing connectivity to this port on remote destinations. Used for advertising a server on the master lists for server browsers.

UDP 27011:
Communicating with the BanList Server from YOUR Server Was formerly 27013 - much in/out traffic too

UDP 27015:
Incoming connectivity to this port (or whatever port the server had been changed to, if not the default). Used for all client/server game traffic (including voice), server info requests, etc.

P2P Applications:

Shareaza
KaZaA Lite
bitTorrent

Emule
Trigger TCP 1024-65535 4661
Incoming TCP 1024-65535 4662
Incoming UDP 1024-65535 4665

APPENDIX E | Technical Specifications

Below is an outline of the Technical Specifications for the Barricade g 2.4 GHz 54 Mbps Wireless Broadband Router with USB Print Server (SMC2804WBRP-G)

Standards
802.3, 802.3u, 802.11b, 802.11g, USB 1.1

WAN Port
1 - 10/100Mbps RJ45, with Auto MDI/MDIX

LAN Port
4 - 10/100Mbps RJ45, with Auto MDI/MDIX

Printer Port
1 – USB 1.1 printer port

Supported WAN type
Static IP
Dynamic IP
PPP over Ethernet
PPTP
Big Pond

NAT
Maximum 253 Users

Protocol
IP Protocol
TCP/IP v4
DHCP server
Proxy DNS server

Management and Configuration
Web-based

Firewall
NAT firewall and SPI firewall

VPN
VPN pass-through including PPTP/L2TP/IPsec

User Authentication
Password protected browser-based UI
PAP/CHAP/MSCHAP Authentication protocol supported

Upgrade method
Web-based

LEDs
Power
WAN
WLAN
LAN
Link
Activity

Security
64/128-bit WEP
Wi-Fi Protected Access™
802.1x

Frequency Band:
802.11g Radio: 2.4GHz
802.11b Radio: 2.4GHz

IEEE 802.11b and g compliant:
11 channels (US, Canada)
13 channels (ETSI)
14 channels (Japan)

Antenna Type
Two Detachable Antennas with SMA Connectors

Antenna Gain
2 dBi

Operating Voltage
3.0V ~ 3.6V

Power
9V, 1000 mA

Operating Temperature
0°~40°C

Humidity
10%~90% non-condensing

Storage Temperature
-40°~70°C

Size
130 x 85 x 32mm
(5.12 x 3.35 x 1.26 in)

Weight
370g (13.05oz)

Compliance
FCC Part 15 Class B, Sec. 15.247 and 15.109
ETS 300 328, ETS 300 826, EN60950 and CE-Mark
CSA/TUV
Industry Canada
DGT

APPENDIX F | Compliances

FCC STATMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or device
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

INDUSTRY CANADA (CANADA)

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.

EC DECLARATION OF CONFORMITY (EUROPE)

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Fructuós Gelabert 6-8, 2o, 4a,
08970 - Sant Joan Despí,
Barcelona, Spain.

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/ EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

RFI

- Limit class B according to EN 55022:1998

Emission:

- Limit class B for harmonic current emission according to EN 61000-3-2/1995
- Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity:

- Product family standard according to EN 55024:1998
- Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ±4 kV, Air Discharge: ±8 kV)
- Radio-frequency electromagnetic field according to EN 61000-4-3: 1996 (80 - 1000 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Electrical fast transient/burst according to EN 61000-4-4:1995(AC/DC power supply: ±1 kV, Data/Signal lines: ±0.5 kV)
- Surge immunity test according to EN 61000-4-5:1995(AC/DC Line to Line: ±1 kV, AC/DC Line to Earth: ±2 kV)
- Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996(0.15 - 80 MHz with 1 kHz AM 80% Modulation:3 V/m)
- Power frequency magnetic field immunity test according to EN 61000-4-8:1993(1 A/m at frequency 50 Hz)
- Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994(>95% Reduction @10 ms, 30%
- Reduction @500 ms, >95% Reduction @5000 ms)

LVD:

- EN60950(A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

SAFTEY COMPLIANCE: Underwriters Laboratories Compliance Statement

Important! Before making connections, make sure you have the correct cord set.

Check it (read the label on the cable) against the following:

The unit automatically matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the rear panel.

Operating Voltage	Cord Set Specifications
120 Volts	UL Listed/CSA Certified Cord Set Minimum 18 AWG Type SVT or SJT three conductor cord Maximum length of 15 feet Parallel blade, grounding type attachment plug rated 15 A, 125 V
240 Volts (Europe only)	Cord Set with H05VV-F cord having three conductors with minimum diameter of 0.75 mm2 IEC-320 receptacle Male plug rated 10 A, 250 V

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlu ßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sind beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der EN 60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8 V, 50-60 Hz nicht über oder unterschreiten sowie den minimalen Strom von 1 A nicht unterschreiten.

    Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt70 dB(A) oder weniger.

APPENDIX G | Technical Support

PHONE

From U.S.A. and Canada (24 hours a day, 7 days a week)

- (800) SMC-4-YOU
- (949) 679-8000
- Fax: (949) 679-1481

From Europe (8:00 AM - 5:30 PM UK Time)

- 44 (0) 118 974 8700
- Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:

- techsupport@smc.com
- european.techsupport@smc-europe.com

Driver updates:

- http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

- http://www.smc.com/
- http://www.smc-europe.com/

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-93-477-4935	Fax 34-93-477-3774
UK:	44 (0) 118 974 8700	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 02 739 12 33	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Switzerland:	41 (0) 1 9409971	Fax 41 (0) 1 9409972
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Northern Europe:	44 (0) 118 974 8700	Fax 44 (0) 118 974 8701
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	27-11 314 1133	Fax 27-11 314 9133
North Africa:	34 93 477 4920	Fax 34 93 477 3774
Russia:	7 (095) 290 29 96	Fax 7 (095) 290 29 96
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-2659-9669	Fax 886-2-2659-9666
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-3-5645-5715	Fax 81-3-5645-5716
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for other contact information, please visit www.smc.com